DEPARTMENT OF DEFENSE

DoD Enterprise Architecture
Business Reference Model

v0.04

20 Aug 2005

By

DoD EA Congruence Community of Practice

TABLE OF CONTENTS

THE DOD EA BUSINESS REFERENCE MODEL

INTRODUCTION

The Federal Enterprise Architecture Business Reference Model (FEA BRM) Version 2.0 was released to agencies on June 12, 2003, to support the FY 2005 budget formulation process. A DoD Supplement was published shortly thereafter. The DoD Supplement incorporates newly defined sub-functions under the Defense and National Security Line of Business and replaces the "TBD" sub-functions in the FEA 2.0 release. Office of Management and Budget (OMB), Circular A-11 guidance, which outlines the requirements and questions in the FY 2005 OMB Exhibits 53 and 300 for IT investments, is available at http://www.whitehouse.gov/omb/egov/b-1-information.html.

The FEA BRM structure is the basis for development of the DoD EA BRM. The DoD EA BRM maps to the FEA BRM Lines of Business and sub-functions, and integrates DoD-specific Lines of Business and sub-functions. The DoD EA BRM uses existing DoD Standards with taxonomies and guidance to relate to FEA BRM elements. The mapping to the FEA BRM provides a pre-established bridge for Exhibit 300 preparation and can be used by the Program Manager to facilitate preparation and submission of budget information to the OMB.

STRUCTURE OF THE DOCUMENT

The document is organized according to the following chapters:

Chapter 1 explains the relationship of the DoD EA BRM to the FEA BRM.

Chapter 2 describes the structure of the DoD EA BRM.

Chapter 3 describes, at a high level, the use of the DoD EA BRM.

Chapter 4 is an analysis of the DoD EA BRM with conclusion and recommendations.

Appendix A contains DoD EA BRM Mission Area definitions, including Warfighter, Business, Intelligence, and Enterprise Information Environment (EIE) Lines of Business and sub-functions.

Appendix B contains FEA BRM Lines of Business and sub-functions definitions.

Appendix C provides the mapping of the DoD EA BRM Warfighter Mission Area elements and their relationship to FEA BRM elements.

Appendix D provides the mapping of the DoD EA BRM Business Mission Area elements and their relationship to FEA BRM elements.

Appendix E provides the mapping of the DoD EA BRM Intelligence Mission Area elements to FEA BRM elements.

Appendix F provides the definitions of the DoD EA BRM Enterprise Information Environment (EIE) Mission Area elements to FEA BRM elements.

CHAPTER 1. RELATING THE FEA BRM TO THE DoD EA BRM

FEA BRM DESCRIPTION

The FEA BRM describes the business of the entire Federal Government. The FEA BRM is organized into four business areas, each of which is subdivided into Lines of Business. The four business areas are Services for Citizens, Mode of Delivery, Support Delivery of Services, and Management of Government Resources, as shown in **Figure 1**. Each Line of Business has sub-functions that further refine the Lines of Business. The Defense and National Security Line of Business under Services for Citizens has three sub-functions: Strategic National and Theater Defense, Operational Defense, and Tactical Defense.
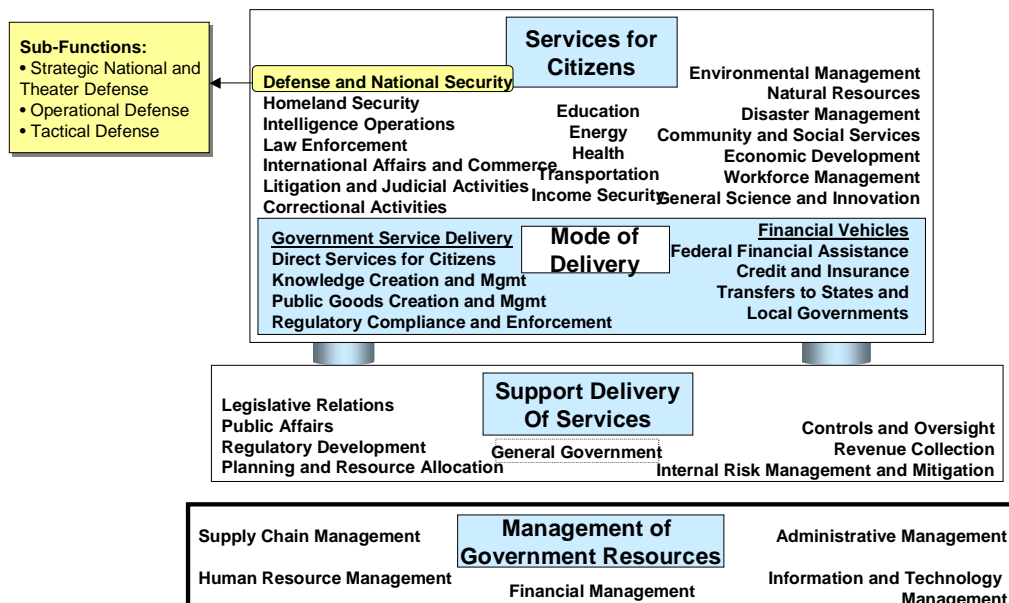
Figure 1. FEA BRM Top Level Structure Showing Business Areas and Lines of Business

Services For Citizens Definition

The Services for Citizens Business Area describes the mission and purpose of the United States Government and more specifically the Department of Defense in terms of the services it provides for, and on behalf of the American citizen. It includes the delivery of citizen-focused, public, and collective goods and/or benefits as a service and/or obligation of the Federal Government to the benefit and protection of the nation's general population and for the Citizens who are a part of the DoD Enterprise.

The Mode of Delivery Definition

The Mode of Delivery Business Area describes the mechanisms the Department of Defense uses to achieve the purpose of government, or its Services For Citizens. It includes Government Service Delivery, such as knowledge creation and management, public goods creation management, regulated activity management, and direct services for the citizen, which includes military operations.

Support Delivery of Services Definition

Support Delivery of Services provides the critical policy, programmatic, and managerial Foundation to support federal government operations.

Management of Government Resources Definition

Management of Government Resources refers to the back office support activities that enable the Department to operate effectively.

DOD EA BRM DESCRIPTION

The following definitions of the DoD sub-functions in the FEA BRM Services for Citizens are based on the DoD Universal Joint Task List (UJTL) top level categories.

DEFENSE AND NATIONAL SECURITY - Protect and advance U.S. national interests and, if deterrence fails, decisively defeat threats to those interests.

- **Strategic National and Theater Defense.** Strategic National and Theater Defense involves establishing national and multinational military objectives; sequencing initiatives; defining limits and assessing risks for the use of military and other instruments of national power; developing global plans or theater war plans to achieve these objectives; and providing military forces and other capabilities in accordance with strategic plans.

- **Operational Defense.** Operational Defense involves linking tactics and strategy by establishing operational objectives needed to accomplish the strategic objectives, sequencing events to achieve the operational objectives, initiating actions, and applying resources to bring about and sustain these events.

- **Tactical Defense.** Tactical Defense involves focusing on the ordered arrangement and maneuver of combat elements in relation to each other and to the enemy to achieve combat objectives.

To fulfill its primary operations providing Strategic National and Theater Defense, Operational Defense, and Tactical Defense, the DoD is involved in many other sub-functions identified in the FEA BRM such as Foreign Affairs, Health Care Services, Criminal Apprehension, Budget Formulation, and Personnel Management. DoD involvement in providing Services for Citizens is usually restricted to providing the service to DoD affiliated citizens, such as health care for military personnel and their families.

Since the DoD is a large business organization, the DoD EA BRM captures the tasks and activities of that large business organization, as shown in **Figures 2, 3, 4, and 5**. The FEA BRM captures the business sub-functions of the entire Federal Government, many of the

tasks and activities in the DoD EA BRM map to sub-functions in the FEA BRM. **Figures 8**, **9**,**10**, and **11** show those sub-functions in the FEA BRM that have tasks or activities in the DoD EA BRM that map to them. Each figure shows one of the four FEA BRM Business Areas. The color- and letter-coded blocks following the sub-function represent the DoD EA BRM mission area where the associated DoD EA BRM task or activity resides. The actual lowest leaf level mappings of the DoD BRM tasks and activities are contained in the Appendices.

Mappings have been made to the Strategic/National set of UJTL categories that, in addition to defense aspects, involve a number of business activities that align with the FEA BRM. The Operational and Tactical categories are believed to be unique to defense, and are thus only mapped to the appropriate top-level defense category in the FEA BRM.

Each DoD EA BRM operational function is related to a FEA BRM sub-function, where possible. DoD professionals needing to align a DoD operation to the FEA BRM for budget submission or other purposes can do so by aligning their operation to the DoD EA BRM, using the DoD EA BRM alignments to the FEA BRM.

CHAPTER 2. STRUCTURE OF THE DoD EA BRM

DOD MISSION AREAS

The DoD provides for the common defense of the United States through Strategic National and Theater Defense, Operational Defense, and Tactical Defense. DoD provides defense through Warfighter Operations supported with Business and Intelligence Operations. The Warfighter, Business, and Intelligence operational functions depend on Information Technology (IT) and other infrastructure. The DoD EA BRM provides a taxonomical structure of DoD operations that gives a cross Department view for Capital Planning and Portfolio Management, aligning IT investments, identifying handoffs and connections, facilitating architecture integration, and other purposes. The DoD operational functions identified in the DoD EA BRM are based on existing DoD standards, i.e., the Universal Joint Task List (UJTL), Business Enterprise Architecture (BEA), NCOW RM, and the Intellligence Community Enterprise Architecture (IC EA).

The DoD EA BRM has four Mission Areas: Warfighter, Business, Intelligence, and Enterprise Information Environment (EIE), each derived from existing DoD standards, as shown in **Figure 1**.
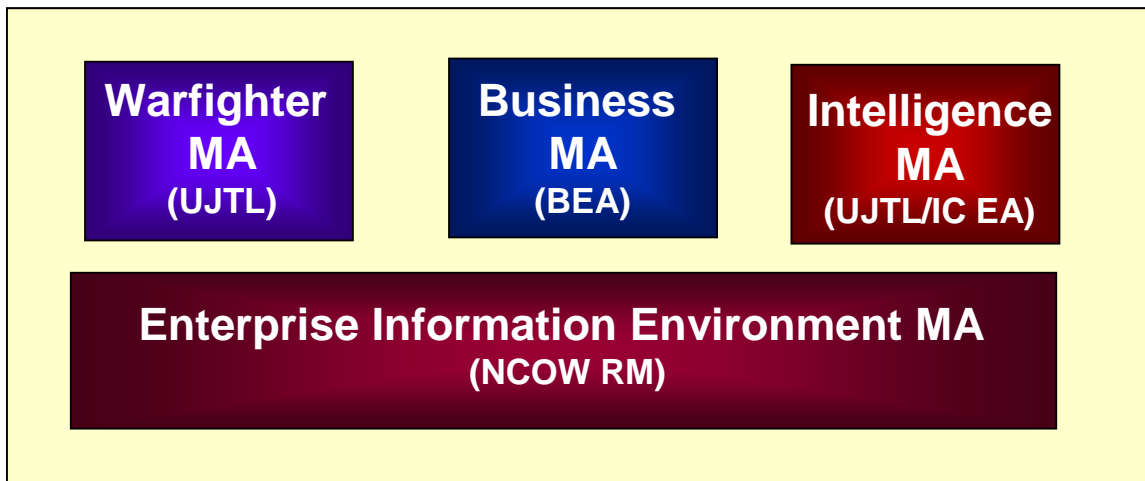
Figure 1. DoD EA BRM Four Mission Areas

Warfighter Mission Area: The DoD UJTL depicts the functions of military operations during engagement of DoD in providing for the common defense. DoD has defined the echelons of defense activities as: Strategic National, Strategic Theater, Operational, and Tactical. These echelons are the top-level categories of the UJTL. The Strategic National UJTL categories include some business, intelligence, and EIE activities.

Business Mission Area: The standard activities contained in the Business mission area are derived from operational activities in the BEA. The DoD Business Management Modernization Program (BMMP) develops and maintains the BEA as a blueprint to guide and constrain investments in DoD organization, operations, and systems as they relate to or impact business operations. The BEA provides the basis for the planning,

development, and implementation of business management systems that comply with Federal mandates and requirements, and produce accurate, reliable, timely, and compliant information for DoD decision makers.

Intelligence Mission Area: The IC EA depicts all functions of intelligence operations, including tasking, posting, processing, and use (TPPU) (per DoD terms) of the intelligence required by consumers for formulating policy, strategy, systems acquisition, and military plans and operations.

Enterprise Information Environment (EIE) Mission Area: The NCOW RM, V1.1, A5 Manage Net-Centric Information Environment depicts the functions of the EIE. The functions include the management of all services and resources to all DoD consumers.

DOD MISSION AREA ACTIVITIES AND TASKS

The DoD EA BRM includes lower level activities or tasks for each top-level item. **Figures 2**, **3**, **4**, and **5** show the detailed activities or tasks for the Warfighter, Business, Intelligence, and EIE Mission Areas, respectively. The definitions for the specific activities in the DoD EA BRM are derived from their authoritative sources and are included in Appendix A. The definitions for the FEA BRM are in Appendix B. Appendices C-F contain tables that map the Warfighter, Business, Intelligence, and EIE BRM elements to the corresponding FEA BRM elements.

WARFIGHTER MISSION AREA

Warfighter Mission Area
(Top Levels)

Strategic National

SN 1 Conduct Strategic Deployment and Redeployment

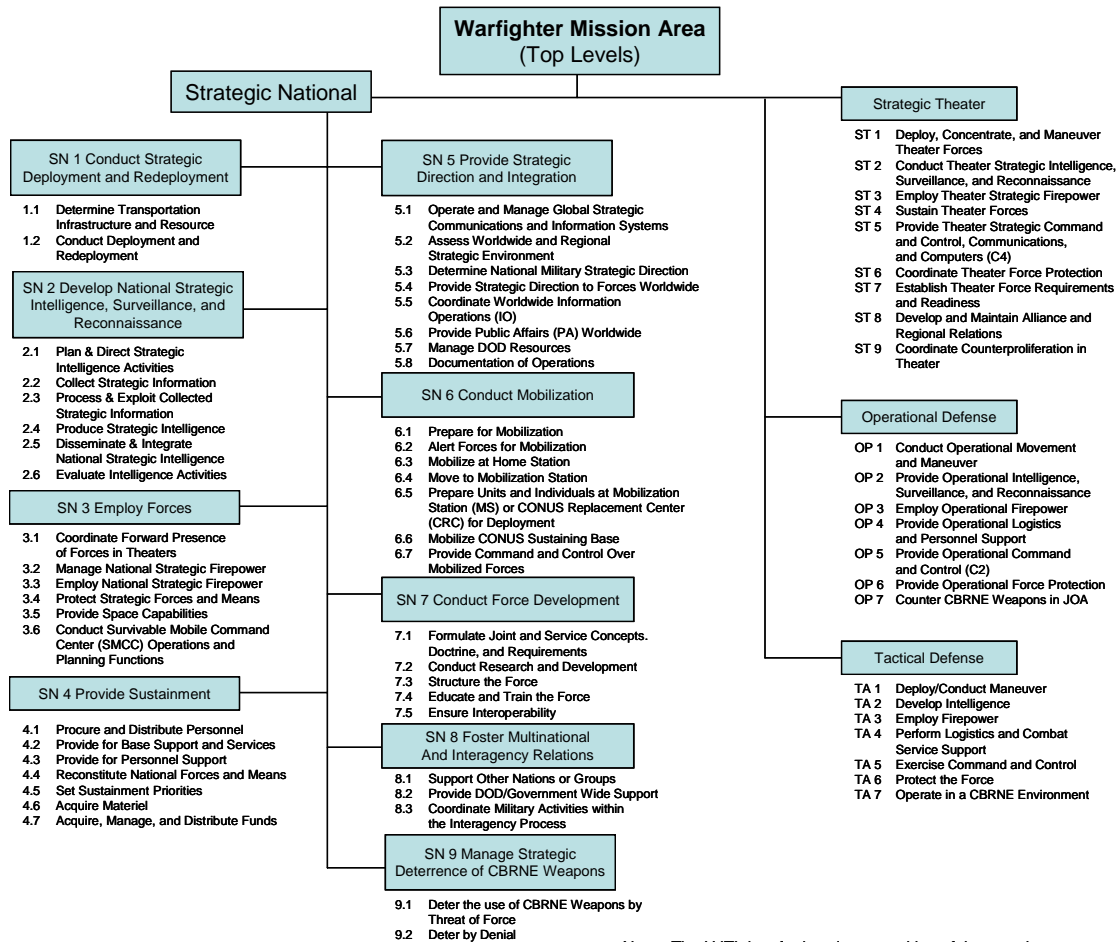1.1 Determine Transportation Infrastructure and Resource
1.2 Conduct Deployment and Redeployment

SN 2 Develop National Strategic Intelligence, Surveillance, and Reconnaissance

2.1 Plan & Direct Strategic Intelligence Activities
2.2 Collect Strategic Information
2.3 Process & Exploit Collected Strategic Information
2.4 Produce Strategic Intelligence
2.5 Disseminate & Integrate National Strategic Intelligence
2.6 Evaluate Intelligence Activities

SN 3 Employ Forces

3.1 Coordinate Forward Presence of Forces in Theaters
3.2 Manage National Strategic Firepower
3.3 Employ National Strategic Firepower
3.4 Protect Strategic Forces and Means
3.5 Provide Space Capabilities
3.6 Conduct Survivable Mobile Command Center (SMCC) Operations and Planning Functions

SN 4 Provide Sustainment

4.1 Procure and Distribute Personnel
4.2 Provide for Base Support and Services
4.3 Provide for Personnel Support
4.4 Reconstitute National Forces and Means
4.5 Set Sustainment Priorities
4.6 Acquire Materiel
4.7 Acquire, Manage, and Distribute Funds

SN 5 Provide Strategic Direction and Integration

5.1 Operate and Manage Global Strategic Communications and Information Systems
5.2 Assess Worldwide and Regional Strategic Environment
5.3 Determine National Military Strategic Direction
5.4 Provide Strategic Direction to Forces Worldwide
5.5 Coordinate Worldwide Information Operations (IO)
5.6 Provide Public Affairs (PA) Worldwide
5.7 Manage DOD Resources
5.8 Documentation of Operations

SN 6 Conduct Mobilization

6.1 Prepare for Mobilization
6.2 Alert Forces for Mobilization
6.3 Mobilize at Home Station
6.4 Move to Mobilization Station
6.5 Prepare Units and Individuals at Mobilization Station (MS) or CONUS Replacement Center (CRC) for Deployment
6.6 Mobilize CONUS Sustaining Base
6.7 Provide Command and Control Over Mobilized Forces

SN 7 Conduct Force Development

7.1 Formulate Joint and Service Concepts. Doctrine, and Requirements
7.2 Conduct Research and Development
7.3 Structure the Force
7.4 Educate and Train the Force
7.5 Ensure Interoperability

SN 8 Foster Multinational And Interagency Relations

8.1 Support Other Nations or Groups
8.2 Provide DOD/Government Wide Support
8.3 Coordinate Military Activities within the Interagency Process

SN 9 Manage Strategic Deterrence of CBRNE Weapons

9.1 Deter the use of CBRNE Weapons by Threat of Force
9.2 Deter by Denial

Strategic Theater

ST 1 Deploy, Concentrate, and Maneuver Theater Forces
ST 2 Conduct Theater Strategic Intelligence, Surveillance, and Reconnaissance
ST 3 Employ Theater Strategic Firepower
ST 4 Sustain Theater Forces
ST 5 Provide Theater Strategic Command and Control, Communications, and Computers (C4)
ST 6 Coordinate Theater Force Protection
ST 7 Establish Theater Force Requirements and Readiness
ST 8 Develop and Maintain Alliance and Regional Relations
ST 9 Coordinate Counterproliferation in Theater

Operational Defense

OP 1 Conduct Operational Movement and Maneuver
OP 2 Provide Operational Intelligence, Surveillance, and Reconnaissance
OP 3 Employ Operational Firepower
OP 4 Provide Operational Logistics and Personnel Support
OP 5 Provide Operational Command and Control (C2)
OP 6 Provide Operational Force Protection
OP 7 Counter CBRNE Weapons in JOA

Tactical Defense

TA 1 Deploy/Conduct Maneuver
TA 2 Develop Intelligence
TA 3 Employ Firepower
TA 4 Perform Logistics and Combat Service Support
TA 5 Exercise Command and Control
TA 6 Protect the Force
TA 7 Operate in a CBRNE Environment

Note: The UJTL has further decomposition of these tasks.

Figure 2. DoD EA BRM Warfighter Tasks (High level)
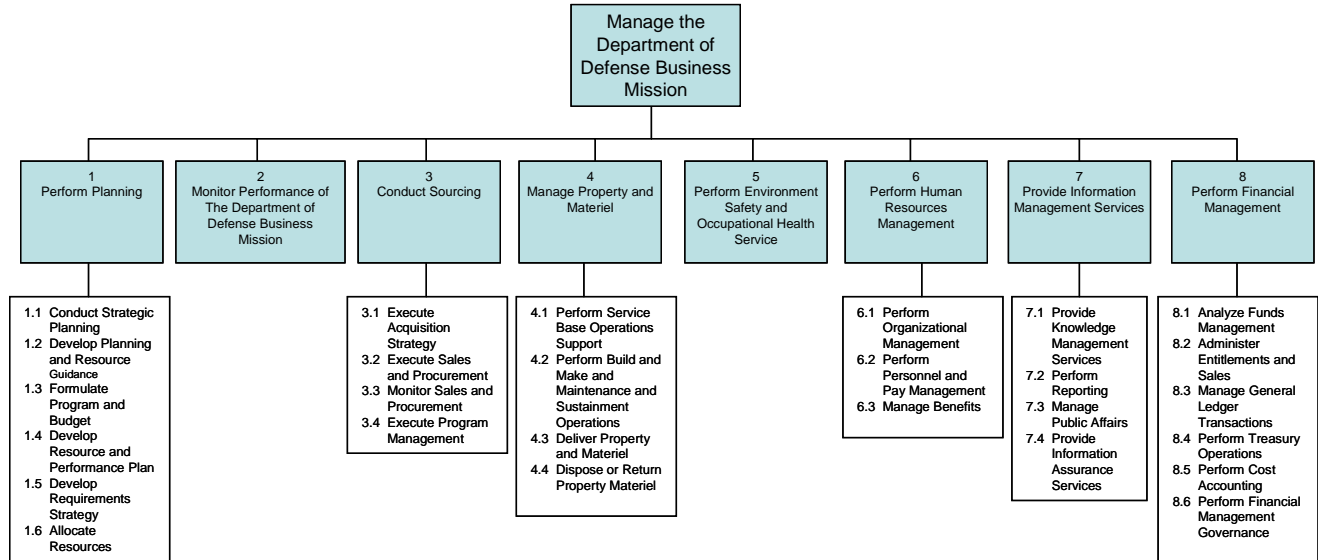
7

BUSINESS MISSION AREA

Figure 3. DoD EA BRM Business Activities
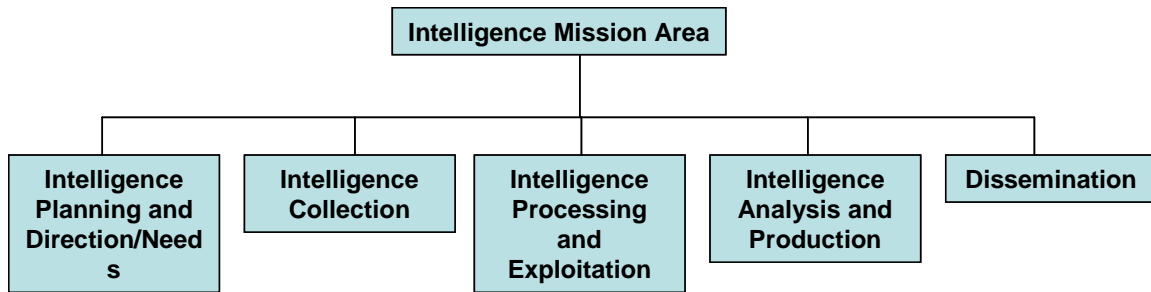
INTELLIGENCE MISSION AREA

Figure 4. DoD EA BRM Intelligence Activities

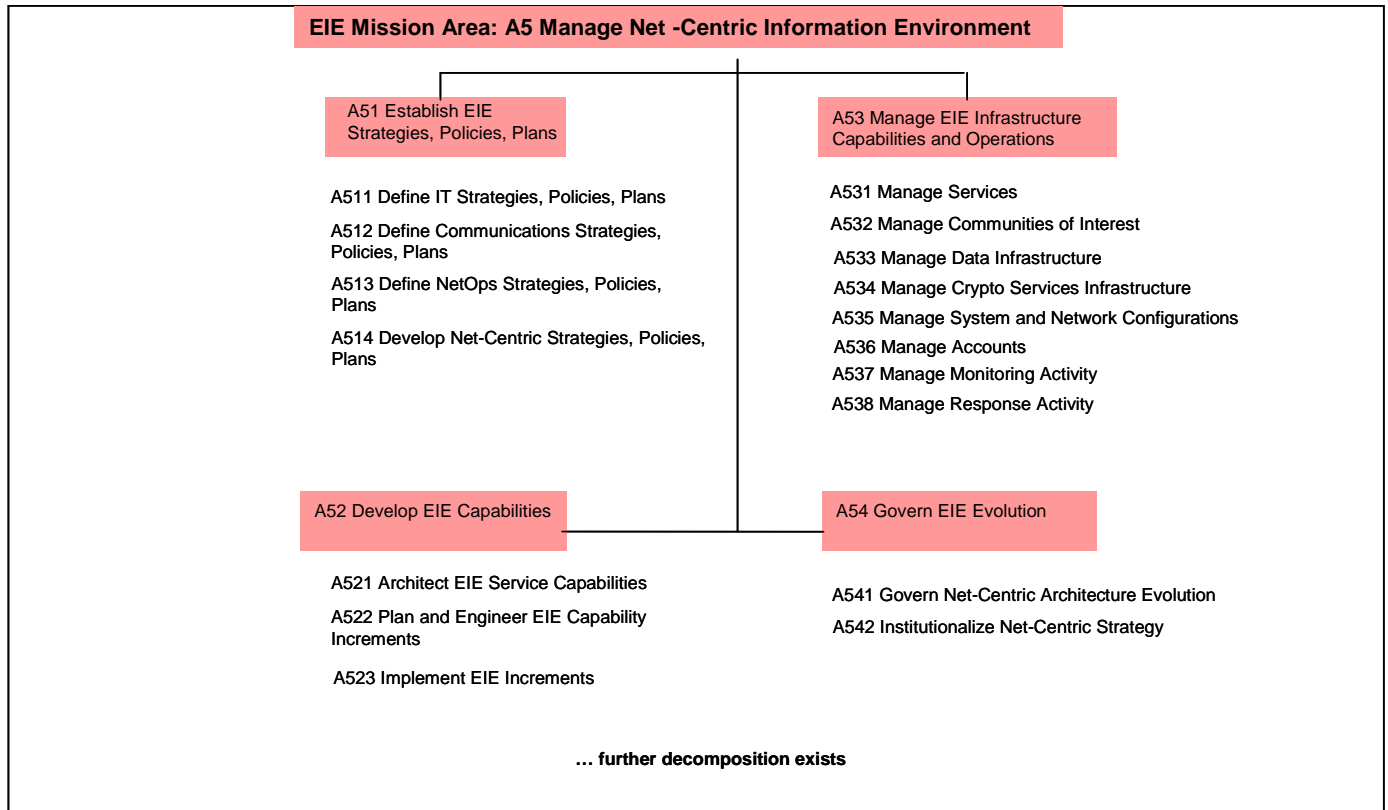## ENTERPRISE INFORMATION ENVIRONMENT MISSION AREA

EIE Mission Area: A5 Manage Net -Centric Information Environment

A51 Establish EIE Strategies, Policies, Plans

A511 Define IT Strategies, Policies, Plans

A512 Define Communications Strategies, Policies, Plans

A513 Define NetOps Strategies, Policies, Plans

A514 Develop Net-Centric Strategies, Policies, Plans

A53 Manage EIE Infrastructure Capabilities and Operations

A531 Manage Services

A532 Manage Communities of Interest

A533 Manage Data Infrastructure

A534 Manage Crypto Services Infrastructure

A535 Manage System and Network Configurations

A536 Manage Accounts

A537 Manage Monitoring Activity

A538 Manage Response Activity

A52 Develop EIE Capabilities

A521 Architect EIE Service Capabilities

A522 Plan and Engineer EIE Capability Increments

A523 Implement EIE Increments

A54 Govern EIE Evolution

A541 Govern Net-Centric Architecture Evolution

A542 Institutionalize Net-Centric Strategy

… further decomposition exists

Figure 5. DoD EA BRM EIE NCOW A5 Activities (NCOW V1.1)

ALIGNMENT OF DOD ACTIVITIES TO THE FEA LINES OF BUSINESS

DoD EA BRM Lines of Business and sub-functions for the Warfighter, Business, Intelligence, and EIE Mission Areas have been identified using the DoD and IC resources described in **Figures 2-5**.

The DoD Warfighter, Business, Intelligence, and EIE Lines of Business align with FEA Lines of Business as shown in **Figures 6-9**. These graphics show the linkage from the four FEA Business Areas to the DoD Mission Areas. The figures are from FEA BRM V1.0 and depict the four areas of the FEA BRM: Services to Citizens, Mode of Delivery, Support Delivery of Services, and Management of Government Resources. The notations, W for Warfighter; B for Business; I for Intelligence; and E for EIE identify where DoD aligns to FEA.

The definitions for all DoD and IC elements are replicated from the authoritative sources and are contained in Appendix A. The definitions for the FEA BRM are contained in Appendix B. Appendices C-F contain the tables that detail the mapping between the Warfighter, Business, Intelligence, and EIE, respectively, and FEA components as shown in the figures. The tables show the mapping from the DoD EA BRM activities and tasks to the FEA BRM sub-functions.

There are overlaps in the mappings between the FEA and the DoD resources. The reason for the overlaps is that, while the definitions derived from the resources may be similar enough for a general mapping, there are differences that need to be analyzed by users for their particular Mission Area. For example, if both Warfighter and Business Mission Areas are designated in a mapping to an FEA Line of Business, the user needs to review and analyze each definition to determine which one most closely fits their Mission Area function.

For a future version, cross organizational functionality can be indicated via a matrix that would indicate functions used by multiple organizations across Mission Areas. This would provide a map to removing redundant systems used to implement the functionality. Also, it would provide a map to business process re-engineering the implementation of cross organizational functionality.

The BRM can then provide one table with a consistent identification scheme, using the six digit number (Business Area, Line of Business, Sub-Function) that is used in budget preparation.

The matrix and table is the next step in establishing a mapping that is an integrated list of functions across the Mission Areas; this work will be undertaken for a future version.

SERVICES FOR CITIZENS

Figure 6 shows the services for the citizen who is a part of the DoD Enterprise, i.e., military personnel and families and DoD employees.   The services that support the citizenry at large are secondary to the primary purpose of the service that is essential for supporting the primary mission of the Department; i.e., **DEFENSE AND NATIONAL SECURITY -** Protect and advance U.S. national interests and, if deterrence fails, decisively defeat threats to those interests.
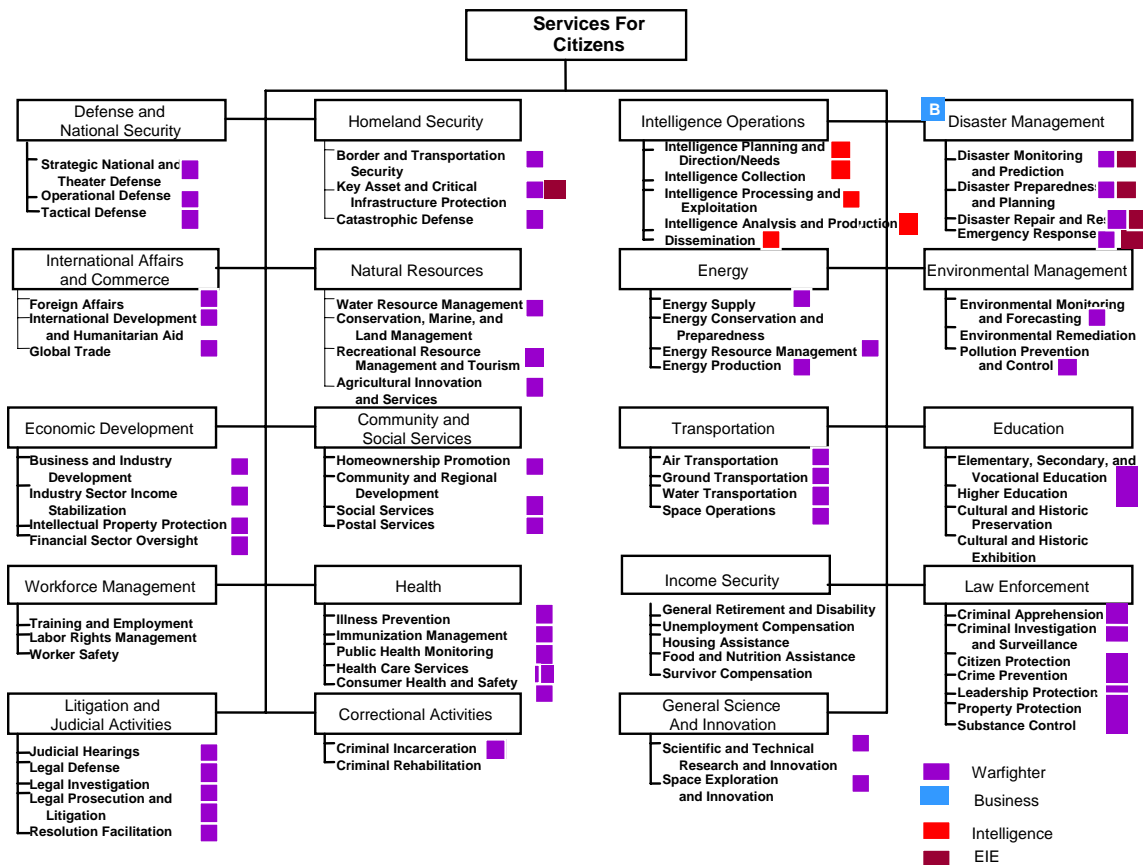

Figure 6. FEA BRM Services for Citizens Sub-Functions that Relate to DoD EA BRM Mission Areas

MODE OF DELIVERY

Mode of Delivery

Government Service Delivery

Support Delivery of Services

Knowledge Creation and Management
- Research and Development
- General Purpose Data and Statistics
- Advising and Consulting
- Knowledge Dissemination

Public Goods Creation and Management
- Manufacturing
- Construction
- Public Resources, Facility & Infrastructure Management
- Information Infrastructure Management

Federal Financial Assistance
- Federal Grants (Non State)
- Direct Transfers to Individuals
- Subsidies
- Tax Credits

Credit and Insurance
- Direct Loans
- Loan Guarantees
- General Insurance

Regulated Activity Management
- Inspections and Auditing
- Standard Setting / Reporting Guideline Development
- Permits and Licensing

Direct Services For Citizens
- Military Operations
- Civilian Operations

Internal Risk Management and Mitigation
- Formula Grants to States
- Project / Competitive Grants
- Earmarked Grants
- State Loans

Legend:
- Warfighter
- Business
- Intelligence
- EIE

Figure 7. FEA BRM Mode of Delivery Sub-Functions that Relate to DoD EA BRM Mission

SUPPORT DELIVERY OF SERVICES
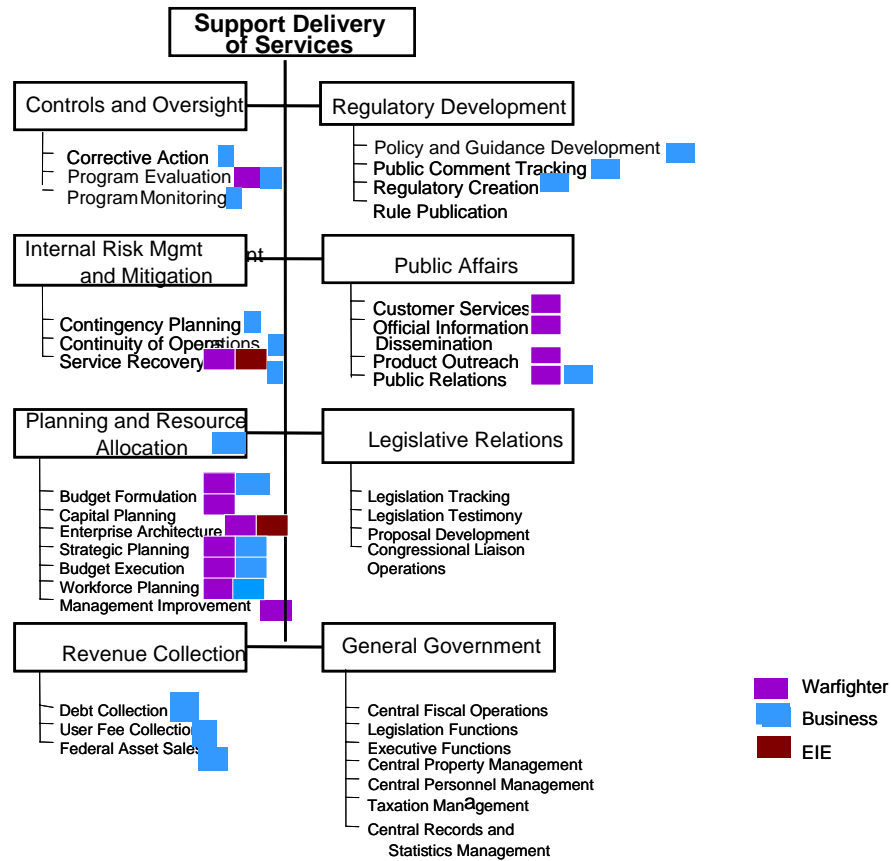
Figure 8. FEA BRM Support Delivery of Services Sub-Functions that Relate to DoD EA BRM Mission Areas

MANAGEMENT OF GOVERNMENT RESOURCES
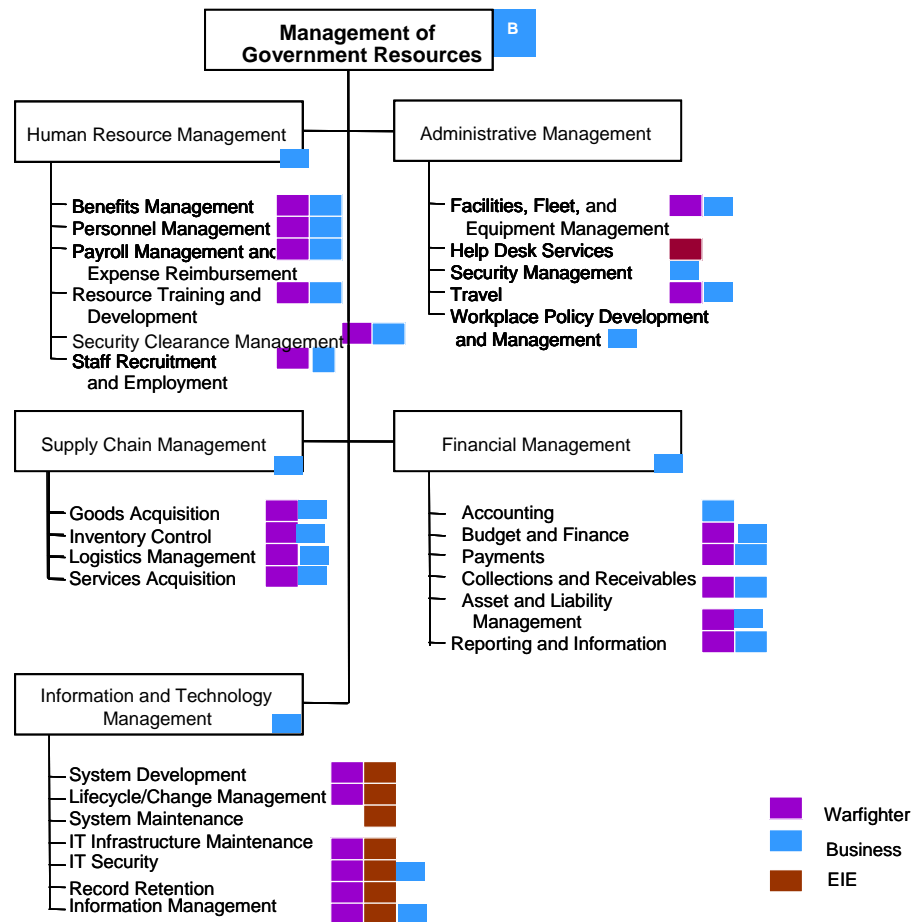
Figure 9. FEA BRM Management of Government Resources Sub-Functions that Relate to DoD EA BRM Mission Areas

CHAPTER 3. USING THE DOD EA BRM

DOD EA BRM GUIDANCE

One of the key features of the President's 2003 E-Government Strategy is the integration of IT investments across agencies around common users of government services and technologies (i.e, individuals, businesses, other governments or federal employees). The DoD EA BRM provides the underlying foundation to support this cross-agency integration of IT investment and service delivery. The "functional" (as opposed to organizational) framework that characterizes the DoD EA BRM provides a new way of thinking about the government's services and the functional commonalities that exist across organizations. These same principles apply to DoD organizations.

While the DoD EA BRM does provide an improved way of thinking about DoD operations, it is only a model; its true utility can only be realized when it is effectively used. The functional approach promoted by the DoD EA BRM will do little to help accomplish the goals of the President's Management Council and the Secretary's transformation agenda if it is not incorporated into the management processes of the Department and OMB. This section summarizes the processes associated with BRM management and use, describes how the BRM will be incorporated into the DoD's annual budget formulation process, and characterizes stakeholder roles and responsibilities.

The DOD EA BRM has two primary classes of customers: agencies external to DoD and the Components, Services, and Agencies within DoD. Each class of customers has different uses for the DoD EA BRM ranging from Capital Planning and Portfolio Management to Business Process Reengineering, Interoperability, and Enterprise Architecture efforts.

The primary value of the DoD EA BRM accrues to the internal user. The DoD EA BRM provides the DoD with an official taxonomy for describing the functional operations of the DoD. These descriptions are independent of any technical implementation. This taxonomy serves as the foundation for many other enterprise level uses including:

1. The DoD EA BRM serves as a lexicon for DoD by facilitating a cross-DoD organizational view of operations based on functional processes, not stovepiped organizational views. This view promotes DoD-level Capital Planning and Portfolio Management, while also providing the overarching structure for the DoD Components, Services, and Agencies to use internally as well.

2. The DoD EA BRM provides the joint-level of a taxonomical structure of DoD operational functions that establishes the hand-offs, connections and/or hooks for the DoD Components, Services, and Agencies to link into with their operational inputs.

3. The DoD EA BRM provides the foundational set of joint-level operational terms for developing DoD architecture products. The use of the DoD EA BRM as an authoritative source of information, useful for the production of operational architecture products, facilitates architecture integration. Varied artifacts may be developed independently, for different reasons and at different levels of granularity, yet all the artifacts will be based on the same common set of terms.

By providing alignment with the FEA BRM, the DoD EA BRM facilitates Capital Planning and Portfolio Management functions at the Federal level.

The OMB budget cycle reviews of Exhibit 300 Reports submitted by DoD Program Managers illustrates how a DoD Program aligns with the FEA BRM activities contained in the Services to Citizens, Mode of Delivery, Support Delivery of Services, and Management of Government Resources sections.

By using the DoD EA BRM, OMB analysts are provided a view of DoD Programs based on a standardized set of functional business and operations criteria at both DoD and Federal levels. It is this level setting of DoD Program activities that facilitate Capital Planning and Portfolio Management at the Federal level.

A two-step process achieves this facilitation. First, programs are compared at the Federal level for possible overlapping of functionality. Second, if two or more programs appear to have duplicate functionality at the Federal level, then a review of the mapped DoD activities would provide an "apples to apples" view of each program's functionality within the operational context in which it resides. It is this operations context view that provides accurate information, in sufficient detail to facilitate Capital Planning and Portfolio Management decisions at both the Federal and DoD levels.

USE OF DOD EA BRM BY KEY STAKEHOLDERS

This section is devoted to describing the various uses of the DoD EA BRM from the point of view of its key stakeholders. It is important to note that this section does not intend to serve as the only guidance that will be issued on the use of the model. Specific guidance on the use of the DoD EA BRM at key times throughout the year will be provided as developed.

Department Of Defense

DoD organizations should use the DoD EA BRM to inform their own EA business architectures and to guide the development and submission of business cases. The result should be improved quality of service at a lower cost.

- DoD organizations should use the DoD EA BRM to describe their operations and to describe the Lines of Business/Internal Functions and Sub-Functions supported by their IT investments.

- DoD determines if other agencies play a role in their Lines of Business/Internal Functions and investigate opportunities for collaboration.

- DoD will use DoD EA BRM and business case information to identify opportunities for cross-agency collaboration.

- Joint business cases are developed and described in terms of the DoD EA BRM and mapped to the FEA BRM.

Using the BRM to Submit Business Cases

Beginning with the President's FY 2005 Budget Preparation process, the DoD along with other Federal agencies, aligned their budget requests with the President's Management Agenda, Federal E-Government initiatives, and the FEA. Specifically relating to architecture, DoD mapped their major IT capital investments to the business lines identified in the FEA BRM, and described how their initiatives supported the FEA BRM Lines of Business and Sub-Functions.

As DoD IT investment requests are being prepared, DoD organizations should use the DoD EA BRM to identify the lines of business that they support. The following table, *Program Manager's Guide to the Appendices,* is a quick look at where to find the information for the mapping between FEA and DoD Lines of Business. The Office of the DoD CIO, building on their Enterprise Architecture work, should then identify the key IT investments that contribute to these lines of business. The DoD CIO should directly, or in conjunction with line of business personnel, review the DoD EA BRM data, as presented in the Federal Enterprise Architecture Management System (FEAMS) to identify other agencies that are performing similar lines of business, and compare their investment requests to the current or planned IT capabilities of the overlapping agency.

Where an opportunity may exist for collaboration, agencies should begin communication prior to the development and submission of their own, separate business cases.

Quick Guide for Program Managers

Program Manager's Guide to Appendices	
Appendix A – DoD EA BRM Definitions	Definitions for Warfighter-related UJTLs, Business Enterprise Architecture (BEA) Activities, Intelligence-related UJTLs, Net Centric Operations and Warfare Reference Model (NCOW RM) V1.1 Activities.
Appendix B – FEA BRM Definitions	Definitions for FEA Lines of Business and sub-functions
Appendix C – Warfighter Tables	Table C-1 Warfighter-related UJTLs to FEA Lines of Business
Appendix D – Business Tables	Table D-1 BEA Activities to FEA Lines of Business
Appendix E – Intelligence Tables	Table E-1 IC EA to FEA Lines of Business
Appendix F – EIE Tables	Table F-1 NCOW RM V1.1 Activities to FEA Lines of Business

Using the BRM to Help Define DoD Business Architectures

DoD organizations should invest time in mapping their business architectures to the DoD EA BRM. This will serve two purposes. First, it simplifies the Exhibit 300 mappings required for budget submissions. Second, it helps DoD organizations identify those areas of the DoD EA BRM and, ultimately, the FEA BRM that require modification. To clarify, if a DoD organization cannot find a proper fit for some of its business processes in the DoD EA RM and if DoD EA BRM cannot find an appropriate fit for its processes in the FEAI BRM, the DoD organization should suggest changes to the models, following the procedure discussed in Chapter 3 of the FEA BRM release document. In this respect, DoD will be improving the utility of the models for itself, the FEA-PMO, and the larger architecture audience.

Using the BRM to Drive Business Line Architectures

As the business-line approach of the BRM begins to take hold in the agencies' capital planning efforts, and as agencies begin to work together along business lines, the FEA-PMO hopes that agencies will begin to drive the direction of these areas of the BRM through the definition of Business Line Architectures. For example, if four agencies are involved in a certain line of business, they will work together to: (1) improve the BRM Sub-Functions; (2) define the desired performance outcomes for the Business Line; (3) design IT solutions that span across their own organizational boundaries; and (4) better serve the citizen.

Using the DoD EA BRM to Submit Joint Business Cases

On August 6, 2002, OMB issued its first guidance on the submission of joint business cases in support of the FY 04 budget process. The guidance related to the revised OMB Circular A-11,

signed by the Director on June 27 of that year, which required that agencies make every attempt to submit joint requests (using the Exhibit 300) that consolidate or align overlapping IT budget requests.

The managing partner (lead agency) will take the lead for the business case and capital asset plan to include managing it through the agency capital planning and budget process and submitting the business case to OMB. The partnering agencies' information on funding and milestones is reflected in the project and funding plan section of Exhibit 300. The project and funding plan will identify all participating agencies, the milestones they are responsible for, and the appropriation/funding source information for the partner agencies.

Partnering agencies will reflect a line item on their Agency IT Investment Portfolio (Exhibit 53) indicating that the funds are part of a multi-agency business case. The description provided on their Agency IT Investment Portfolio will describe where to find the business case in the managing partner's budget submission. Partnering agencies should ensure that their collaboration is indicated in the appropriate sections of the business case before it is submitted to OMB.

Other Users of DoD EA RMs

The DoD EA BRM can significantly improve DoD services by highlighting opportunities that integrate agency operations and IT investments along common Lines of Business within DoD and across the government at large. The DoD EA BRM also illustrates where multiple organizations (and their IT investments) support common Lines of Business in DoD and the government at large.

OMB is responsible for ensuring that government agencies playing a role in the same Lines of Business are not creating duplicative technology investments to meet similar business needs.

OMB will use the FEA to analyze investments in IT to identify:

- Which agencies share common business functions, processes, and activities

- What budget requests support duplicative business functions and information systems

- Where the government is investing money on redundant capabilities, including work under the human capital strategy

- How IT investment is supporting the achievement of performance goals

Each year, OMB will analyze the BRM to identify areas of the BRM that will benefit from cross-agency collaboration and warrant the submission of joint (multi-agency) Exhibit 300s. Each September, once agencies have submitted their budget requests, OMB analysts will map all IT investment business cases (Exhibit 300s) against the DoD EA BRM to identify possible redundancies and additional opportunities for collaboration.   OMB budget examiners will leverage these mappings during the fall review process to facilitate their own cross-agency analyses and to determine the best way to invest funds to achieve performance outcomes. The result will be the identification of opportunities to save money by taking advantage of the economies of scale offered by cross-organizational collaboration and to improve and simplify the delivery of services to the citizen.

CHAPTER 4. ANALYSIS

DOD EA BRM PURPOSE

Due to the unique mission requirements of the DoD to provide for the common defense of the United States by conducting Strategic National and Theater Defense, Operational Defense and Tactical Defense, the DoD is functionally structured to support its Warfighting Operations with Business and Intelligence Operations. In today's and tomorrow's technological environment, DoD foresees a net centric approach to conduct these functions.

The DoD EA RM has a dual primary purpose. First, it provides the model of these functions as part of the DoD Enterprise Architecture. The content of this model is derived from four sources: the DoD UJTLs for conducting Joint Military Operations, the DoD BEA, input from the DoD Intelligence Community, and the DoD NCOW RM V1.0. The second primary purpose is that the DoD EA BRM provides the official DoD mapping to FEA BRM.

The mapping between the DoD EA BRM and the FEA BRM, contained in the DoD EA BRM, is the essential cross-walk that provides the basis for the Federated relationship between the business and operational segments of the FEA and the DoD EA.

The DoD EA BRM is intended to be utilized by DoD to better align IT investments in direct support of the four strategic risk areas identified in the 2003 Annual Defense Report by the Secretary of the Department of Defense to the President and Congress: Force Management Risk, Operational Risk, Institutional Risk, and Future Challenges Risk. This alignment of investment in IT is facilitated in the DoD EA BRM by mappings between DoD Operations to the Lines of Business and Sub-Functions performed by the Federal Government, independent of the agencies that perform them. The mapping facilitates a common understanding between the Federal Government's business for agencies, oversight bodies, IT decision makers, and other stakeholders; and DoD's operational structure.

CONCLUSION

The primary focus for the development of the DoD EA BRM was to address the DoD requirements of establishing a standardized mapping between DoD business processes and the FEA BRM. The purpose of this mapping was to facilitate accuracy in the DoD IT budget for Capital Planning and Portfolio management at the Federal level.

The evolution of the DoD EA BRM should be configuration-managed by the office of the DoD CIO with DoD Component, Services, and Agencies (C/S/As) input. This evolution will solidify and expand the functionality of the DoD EA BRM by addressing the areas identified by the DoD EA Congruence Community of Practice in the Lessons Learned document.

PROPOSED CHANGES TO THE DoD EA BRM

The OV-5 Operational Activities in BEA v2.2 were domain oriented; that is, they were developed from the organizational perspective of domains. The OV-5 Operational Activities in BEA v2.3 are developed from an enterprise wide business function perspective that is not dependent on organizational structure. This provides a more stabile architecture because business functionality is less susceptible to change than organizational structure. Consequently, BMMP has developed a new node-tree for BEA v2.3 that has the following level A0 Operational Activities:

- Perform Planning
- Conduct Sourcing
- Manage Property and Material
- Perform Environment Safety and Occupational Health Services
- Perform Human Resources Management
- Manage Information
- Perform Financial Management

BMMP is in the process of establishing the linkages between these level A0 Operational Activities and lower level Operational Activities, and the linkages between these Operational Activities and other DoDAF products such as the SV-4 System Functions and the OV-6c Processes.

APPENDIX A -- DoD EA BRM DEFINITIONS

DOD EA BUSINESS REFERENCE MODEL DEFINITIONS

This section of the DoD EA BRM contains the definitions used to map the FEA BRM elements to the DoD EA BRM elements. There are four sets of definitions. Note that the FEA BRM definitions are in the body of the document.

- Warfighter Operations: definitions include the Strategic National activities derived from the Universal Joint Task List.
- Business Operations: definitions include the Business Enterprise Architecture (BEA) activities from the OV-5.
- Intelligence Operations: definitions include the intelligence activities derived from the IC EA that relate to DoD intelligence organizations (Defense Intelligence Agency, National Security Agency, Service intelligence organizations).
- Enterprise Information Environment: definitions include the Net-Centric Operations and Warfare Reference Model A5 activities that relate to Lines of Business elements.

These definitions may be used as a reference for reviewing and analyzing the tables in the Warfighter Operations, Business Operations, Intelligence Operations, and the Enterprise Information Environment appendices.

WARFIGHTER OPERATIONS DEFINITIONS FOR DOD EA BRM

This section contains definitions of Universal Joint Task List (UJTL) activities that map to the FEA BRM. The definitions may be used as a reference for the tables in Appendix A that map the FEA BRM to the DoD EA BRM.

- **SN 1 Conduct Strategic Deployment and Deployment** - To conduct the relocation of forces to desired theaters and their return in accordance with national military strategy and OPLANs to include within CONUS in support of Homeland Security missions. This task focuses on the movement of forces and resources from a point of origin to a specific operational area. Strategic deployment encompasses relocation of forces, equipment, and supplies to a theater from CONUS, or from one theater to another, for subsequent reception, staging, onward movement, and integration (RSOI). This task applies to mobilization and nonmobilization situations. Forces include air, land, and sea forces, as well as special operations forces.

- **SN 2 Develop National Strategic Intelligence, Surveillance, and Reconnaissance** -To produce the intelligence required by strategic consumers for formulating national-level policy, strategy, systems acquisition, and military plans and operations. The strategic intelligence task applies across the range of military operations including military operations other than war. This task includes providing national strategic surveillance and reconnaissance.

- **SN 3 Employ Forces** - To employ forces to achieve desired end states to include within the United States if in response to homeland security. Employment at the strategic national level includes the commitment of functional combatant command assets or other forces under direct supervision of the Secretary of Defense to execute a national mission. This task includes efforts that integrate two or more theater strategies or US and multinational national-level efforts. It also includes coordination and integration of non-DOD support to combatant commands and DOD support of non-DOD agencies and other nations and groups.

- **SN 4 Provide Sustainment -** To maintain the necessary level and duration of military activity to achieve national and multinational objectives. This task includes providing, maintaining, transporting, or assisting/coordinating those levels of force, personnel, materiel, and consumables necessary to support the national and/or multinational military strategy. In military operations other than war, this task pertains to support of US forces and agencies and to provide advisory and training assistance to a host-nation.

- **SN 5 Provide Strategic Direction and Integration** - To develop and revise national and/or multinational military strategy. This task is based on national security strategy for the attainment of strategic security interests, objectives, and end states. The Joint Chiefs of Staff (JCS) (includes the Chairman and Vice Chairman of the Joint Chiefs of Staff) derives strategic direction from national security strategy and policy directives. The Secretary of Defense, through the Chairman of the Joint Chiefs of Staff, provides strategic guidance and direction to the combatant commanders. The combatant commanders subsequently provide strategic direction for the employment of joint, Service, supporting, special, and multinational forces through their unified action in theater strategies and campaign plans. This task includes providing clear command relationships and tasking authority through an appropriate JCS planning, warning, alert, or execute order. Theater operations are often in conjunction with interagency, nongovernmental, and private voluntary organizations and United Nations forces. These three strategies (national security, national military, and theater) and related strategic plans integrate the national ends, ways, and means. Includes missions in support of homeland security within the United States.

■ **SN 6 Conduct Mobilization** - To expand the Armed Services by assembling and organizing national resources to support national objectives in time of war or other emergencies. This task brings the Armed Services, or part of them, to a state of readiness for war or another national emergency. This task includes advising the Secretary of Defense on mobilization. It includes activating all or part of the Reserve Components (RC), as well as assembling and organizing personnel, supplies, and materiel. This task is performed when the Secretary of Defense initiates a selective, partial, full, or total mobilization. Mobilization tasks of combatant command components are included under this joint task. For example, US Army Pacific (USARPAC), a component command of US Pacific Command (USPACOM), has mobilization responsibilities. These mobilization responsibilities are analyzed under the national strategic level (rather than a theater strategic task) because USARPAC performs these responsibilities as a major Army command (MACOM). Thus, USARPAC is considered to be performing national military functions. However, USARPAC reports mobilization status through the combatant command as well as the Service. For demobilization, reverse SN 6.5, SN 6.6, and SN 6.7.

■ **SN 7 Conduct Force Development** - To translate projected Military Department, Service, and USCINCSOC resources—manpower, fiscal, and materiel—into time-phased programs and structure (expressed in dollars, equipment, and units) needed to accomplish national security, national military, multinational (alliance and coalition), and theater strategy, and Service-assigned missions, core competencies, and functions.

■ **SN 8 Foster Multinational and Interagency Relations** - To work within the Interagency process and with representatives of other nations and regional organizations. This task ensures the accomplishment of US politico-military objectives through the combined action of different US organizations and friends, allies, neutrals, and other nations overseas. Includes missions in support of homeland security within the United. States.

■ **SN 9 Manage Strategic Deterrence of CBRNE Weapons** - To deter the use or the threatened use of CBRNE weapons, and to prevent or deny an adversary any advantage over U.S. Forces, or our friends and allies, by the use of CBRNE weapons. This includes the full range of military, political, economic and diplomatic tools to also prevent, constrain, or reverse the proliferation of CBRNE weapons. Activities include both proactive and reactive elements so that in the event deterrence fails, our forces maintain the ability to operate in a CBRNE weapons environment without significant degradation.

BUSINESS OPERATIONS DEFINITIONS FOR DOD EA BRM

Standard Business Activities and Descriptions

This section contains the standard business activities and their definitions. Activities are grouped according to the Business Domain that "owns" them, with the addition of Financial Management and Reporting (FMR) and Business Support categories containing required activities not currently owned by a Domain. The definitions may be used as a reference for the tables in Appendix D that map the FEA BRM to the DoD EA BRM.

0 Manage the Department of Defense Business Mission
This activity supports the Department of Defense business mission areas that deal with all aspects of planning, acquiring, using and disposing, terminating, or separating of goods and services, assets and human resources through accurate financial management, asset management and human resource management.

1 Perform Planning
This activity determines, identifies, establishes, and allocates strategic direction, identifying and establishing defense programs and processes, and allocating resources (capital and labor) among those programs and processes to perform DoD's mission.

1.1 Conduct Strategic Planning
This activity develops strategic goals, objectives and the associated products to achieve the organization's mission for a specified time period. These are reflected in strategic plans, capabilities, and assessments.

1.2 Develop Planning and Resource Guidance
This activity produces direction or policy for the business activities based on the strategic goals and objectives.

1.3 Formulate Program and Budget
This activity generates and revises requisitions and implements buying contract/orders and sales contract/orders at all levels (contract, call, line item).

1.4 Develop Resource and Performance Plan
This activity translates strategic plans, guidance, and requirements into detailed plans to execute programs and to describe what business activities will be executed and what is the expected outcome. This activity also develops the resource and performance plan to achieve specific business operations and program goals, objectives, and performance. Plans are maintained and updated based upon receipt of the program and funding document, management reviews, fact of life changes, or contingency operations. Plans describe business programs in terms of performance levels, outcomes, and expected risks.

1.5 Develop Requirements Strategy
This activity assesses requirements and develops strategies to acquire or source these requirements, including forecasting costs, identifying risks, and any related selection or negotiation criteria.

1.6 Allocate Resources
This activity distributes approved DoD resources or adjustments (e.g., reprogramming and supplemental) within guidelines provided by statute, policy, and regulation. This includes distribution of resources from OSD to DoD components and subsequent distribution to lower echelon commands down to the lowest level designated.

2 Monitor Performance of the Department of Defense Business Mission
This activity measures progress towards satisfying the strategic objectives of the Department of Defense Business Mission.

3 Conduct Sourcing
Once the plan identifies potential providers, solicitation strategies and establishes selection criteria, this activity establishes sourcing vehicles, requests proposals, reviews bids, selects

providers and issues contracts. This activity also tracks, monitors and closes out contracts and ensures that vendors and/or service providers are meeting terms and conditions and other requirements. Finally, this activity is responsible for executing acquisition business plans of Department of Defense by managing programs.

3.1 Execute Acquisition Strategy

This activity matches requirements to existing Sourcing and/or Enterprise Contract/Agreements. Enterprise implies multiple vendor options whereas Sourcing is typically for a particular program/vendor (e.g. F18/Boeing). If a new Sourcing or Enterprise Contract/Agreement is required, the requirement to be fulfilled is communicated as a Solicitation, Request for Information, Request for Quote, or Request for Proposal. This activity also includes the evaluation and/or negotiation of proposals resulting in the issuing of a Sourcing or Enterprise Contract/Agreement.

3.2 Execute Sales and Procurement

This activity generates and revises requisitions and implements buying contract/orders and sales contract/orders at all levels (contract, call, line item).

3.3 Monitor Sales and Procurement

This activity reviews contracts and other information to ensure that buying contract/orders and sales contract/orders compliance has been achieved. Internal and external vendors and/or service providers performance, service deliveries, periods of performance, payment reconciliation and contract closure are all reviewed.

3.4 Execute Program Management

This activity manages the elements of the program's resources and risk, integrates government and contractor efforts, and reports program status and issues.

4 Manage Property and Materiel

This activity includes all activities associated with the management and movement of materiel and assets throughout the lifecycle from procurement/acquisition, production, end use and maintenance/sustainment to final disposition.

4.1 Perform Service Base Operations Support

This activity consists of activities that enable the performance of both common and asset level installation support functions including real property services (e.g. space management, utility services, pest control services, pavement clearance services, custodial services, refuse collection, grounds maintenance services, etc), housing management, and common installation support such as BRAC, certain on-base transportation, and other common support services.

4.2 Perform Build and Make and Maintenance and Sustainment Operation

This activity is associated with developing Plant Property and Equipment assets, maintaining them in standard working condition, and extending their capacity, capability, or useful life. Examples of these activities include construction of buildings and facilities and production of equipment, as well as repair, overhaul, restoration, and modernization of these assets.

4.3 Deliver Property and Materiel

This activity satisfies the needs of internal and external customers, as evidenced by orders (i.e. requisitions, purchase orders or contracts), by issuing or transporting inventory and related materials, or capital equipment. Materiel and equipment come under control of the Deliver activity when they are received at the warehouse. The Deliver activity is triggered when an inquiry or order is received from a customer. It includes the care and custody of the goods, picking orders, arranging transportation and issuing or shipping the goods. The Deliver activity is complete when the goods have been received by the consignee, acknowledged and invoiced, and the intransit record has been cleared.

4.4 Dispose or Return Property and Materiel

This activity sends goods and equipment back into the supply chain when they are received in error, in excess of required quantities, or defective obsolete, damaged, or worn rendering them no longer useful in their current condition. This activity also includes the disposal of real property by demolition or transfer.

5 Perform Environment Safety and Occupational Health Service

This activity refers to distinct business areas within DoD that address environmental quality, restoration, range sustainability, occupational health, safety. While each program within these business areas operates in accordance with specific laws, regulations, DoD guidance, service level guidance and best practices, there are sets of common activities operating across these areas. Common activities include identifying and understanding the environment, safety, health or readiness issues, risk assessment, developing solutions, implementing solutions, developing agreements and the conduct of monitoring. Specific business areas addressed are Compliance; the area of environmental management that ensures effective and efficient compliance with existing Federal, host nation, state and local environmental laws and regulations, Pollution Prevention (P2); which seeks to eliminate or reduce pollution at its source and promote recycling. P2 programs are the preferred means of achieving environmental compliance, protecting human health and reducing the use of hazardous materials, and decreasing the volume of solid waste. Conservation; which balances the responsibility of protecting cultural and natural resources with the requirements of military mission support., Clean-up/Restoration; the identification, investigation, research and development, and cleanup of contamination from hazardous substances, pollutants and contaminants and the correction of other environmental damage such as detection and disposal of unexploded ordnance (UXO), which creates an imminent and substantial endangerment to the public health or welfare or to the environment, Safety; which ensures that the Warfighter and the supporting personnel work in an environment that is free from occupational hazards such as improper machine operation, faulty equipment, and other safety related issues, and Occupational/Environmental Health; which ensures that the Warfighter, supporting personnel, and other stakeholders are protected from various health issues that can arise during normal operations

6 Perform Human Resources Management

This activity encompasses all activities associated with entry to/exit from the organization; career development and management; benefits, travel and pay management; and execution of human resource policies, procedures and employee information management.

6.1 Perform Organizational Management

This activity encompasses all activities associated with managing the human resources infrastructure for Department of Defense (DoD) organizations. This infrastructure supports DoD legal programs, law enforcement programs, individual travel and organizational structures with position specifications. This activity includes managing the implementation of DoD mission plans by formulating force structure, strength projections, accession targets and distributing peacetime authorizations and wartime requirements

6.2 Perform Personnel and Pay Management

This activity encompasses all activities associated with entry to/exit from the organization; profile record management; career development and management; execution of human resources policies, procedures, and employee information (profile record and workforce communication) management; and administering, authorizing and calculating pay. This activity includes the following: accession, recruitment, strength management, placement and assignment, position fill management and classification, budget justification, resource utilization projection, adverse action, personnel actions, social actions (including Equal Employment Opportunity programs), personnel administration support, personnel security investigations and clearances, time and attendance tracking, human resources reporting, transition of member/employee, education, training and development, competency management, performance review and administration (including the promotion process). This activity also includes pay administration and policy, leave calculation, annuitant and retirement pay, special pay and entitlements, pay authorization and calculation, pay adjustments, allotments, bonds, garnishments and offsets, Thrift Savings Plan calculation, payroll and tax reporting, travel pay and other reimbursables.

6.3 Manage Benefits

This activity is associated with the management of benefits to support Department of Defense Quality of Life programs. This activity also includes indirect compensation, wage supplements, indirect payments, and provision of Morale, Welfare, and Recreation Programs (including Chaplain programs, commissary, exchange, and other Non-Appropriated Fund (NAF) operations). This includes medical, dental, life and long-term insurance; pension/retirement; flexible spending; disability benefits; entitlements; benefits eligibility, including management of housing and educational benefits, enrollment and termination; tracking of health care administrators; savings management (Thrift/Bonds); and benefits reporting.

7 Provide Information Management Services

This activity involves the coordination of information resources to support or provide a service for or to an organization and its components or users. Information Management Services involves the coordination of information collection, storage, and dissemination and destruction.

7.1 Provide Knowledge Management Services

This activity formalizes the management and leveraging of intellectual assets. Knowledge Management is an enterprise discipline that promotes a collaborative and integrated approach to the creation, capture, organization, access and use of information assets, including the tacit, uncaptured knowledge of people. This activity involves programs and activities in which the federal government creates or develops a body or set of knowledge, the manipulation and analysis of which can provide inherent benefits.

7.2 Perform Reporting

This activity includes the process of receiving financial and management reporting requirements, preparing the information product, and distributing the finished product to the requestor. The activity distributes information in a specified format for analysis and decision-making. This activity routinely involves summarizing and clearly communicating information collected through various means and providing output results based on specified reporting requirements such as format, frequency and type

7.3 Manage Public Affairs

This activity involves the exchange of information and communication between the Federal Government, citizens and stakeholders in direct support of citizen services, public policy, and/or national interest.

7.4 Provide Information Assurance Services

This activity provides the basis for services that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This activity also provides for restoration of information systems by incorporating protection, detection, and reaction.

8 Perform Financial Management

This activity measures, operates and predicts the effectiveness and efficiency of the Department's financial activities in relations to its financial objectives, and includes the responsibility for establishing financial policies, practices, standards and ensuring a system of controls exists that reliably captures and reports activity in a consistent manner.

8.1 Analyze Funds Management

This activity manages funds that have been allotted by business plan and tracks subsequent execution of funds by monitoring commitments, obligations, and expenditures.

8.2 Administer Entitlements and Sales

This activity encompasses fund validation activities at both the commitment and obligation stages, as well as accounts payable activities associated with commercial pay operations. This activity further encompasses the management of all claims receivable accounts owed to the Department of Defense. This activity also includes the management of accounts receivable related to the sales of goods or services, to include the generation of a billing document.

8.3 Manage General Ledger Transactions

This activity encompasses accounting for assets, liabilities, fund balances, revenues and expenses associated with the maintenance of federal funds and expenditure of federal appropriations (salaries and expenses, operation and maintenance, procurement, working capital, trust funds, etc.). In accordance with applicable federal standards (FASAB, Treasury, OMB, GAO, etc.) the activity also includes posting all financial transactions to the general ledger, as well as the closing and review processes.

8.4 Perform Treasury Operations

This activity processes disbursements, collections, returns and replacement financial instruments and delinquent receivables for the Department of Defense. This activity also involves the management of securities held for the production of investment revenues, net of premiums and discounts.

8.5 Perform Cost Accounting

This activity provides for the assembling and recording of all the elements of cost incurred to accomplish a purpose, to carry on an activity or operation, or to complete a unit of work or a specific job.

8.6 Perform Financial Management Governance

This activity creates, maintains and disseminates policies, requirements and other directives governing the performance of financial management activities.

INTELLIGENCE OPERATIONS DEFINITIONS FOR DOD EA BRM

The IC EA Coordination Draft of April 2004 defines the Intelligence LOB as follows:
The Intelligence LOB is decomposed into five Subfunctions. These sub-functions provide a reference point from which the IC can identify supporting information, applications and technologies across the community. At a later date, these sub-functions may be further decomposed as necessary to support analyses and development. The sub-functions are:

- **Intelligence Planning and Direction/Needs**: Establishing the intelligence requirements of the policymakers-The President, the National Security Council, military commanders, and other officials in major departments and governmental agencies.

- **Intelligence Collection**: Gathering of raw data from which finished intelligence is produced.

- **Intelligence Processing and Exploitation**: Conversion of large amounts of data to a form suitable for the production of finished intelligence to include translation, decryption, and interpretation of information stored on film and magnetic media through the use of highly-refined photographic and electronic processes.

- **Intelligence Analysis and Production**: Integration, evaluation, and analysis of all available data and the preparation of a variety of intelligence products.

- **Dissemination**: Delivering the intelligence products to consumers.

ENTERPRISE INFORMATION ENVIRONMENT DEFINITIONS FOR DOD EA BRM

This section contains definitions of A5, Manage Enterprise Information Environment activities that map to the FEA BRM. The definitions are from NCOW RM V1.1 Draft Integrated Dictionary. The definitions may be used as a reference for the tables in Appendix D that map the FEA BRM to the DoD EA BRM. Note that the definitions contain only the A5 *Manage Net-Centric Information Environment* activities of the NCOW RM V1.1 because this set of activities directly relates to lines-of-business.

A5 Manage Enterprise Information Environment: This activity consists of the planning, organizing, coordinating, and controlling the establishment, maintenance, and dissolution of all the capabilities of and services provided by the information environment. It comprises the development of the environment's capabilities, the management of its system and network configurations, as well as the conduct of its administration, monitoring, and response activities. It also consists of performance of all NetOps activities necessary to manage and protect the flow of information within the information environment. These activities are performed by NetOps Personnel. It takes functional and operational performance requirements as inputs and produces operational capabilities within the information environment. This activity is controlled by the operational environment; plans; policies; guidance; laws and regulations; tactics, techniques, and procedures; standards; and funding. It is enabled by Global Information Grid (GIG) systems and networks; net-centric enterprise services; net-centric Community of Interest (COI) applications and services; GIG NetOps facilities; and GIG NetOps personnel.

A51 Establish EIE Strategies, Policies, and Plans: This activity establishes current and future EIE goals, objectives, and implementing plans and procedures, and assigns roles and responsibilities for EIE modernization, operations, sustainment, and readiness including integrated EIE portfolio investment management. Outputs of this activity provide the EIEMA oversight authorities the basis for measuring EIE-related activity performance at all levels of the enterprise.

A511 Define IT Strategies, Policies, and Plans: This activity establishes current and future IT goals, objectives, and implementing plans and procedures, and assigns roles and responsibilities for all IT modernization, operations, sustainment, and readiness including IT portfolio investment management. Outputs of this activity provide the EIEMA oversight authorities the basis for measuring IT-related activity performance at all levels of the enterprise.

A512 Define Communications Strategies, Policies, and Plans: This activity establishes current and future communications goals, objectives, and implementing plans and procedures, and assigns roles and responsibilities for all communications modernization, operations, sustainment, and readiness including communications portfolio investment management. Outputs of this activity provide the EIEMA oversight authorities the basis for measuring communications-related activity performance at all levels of the enterprise.

A513 Define NetOps Strategies, Policies, and Plans: This activity establishes current and future NetOps goals, objectives, and implementing plans and procedures, and assigns roles and responsibilities for all NetOps modernization, operations, sustainment, and readiness including NetOps portfolio investment management. This activity integrates the operational aspects of systems and networks, communications, IT, IA, and content-staging strategies, policies, and plans. Outputs of this activity provide the EIEMA oversight authorities the basis for measuring NetOps-related activity performance at all levels of the enterprise.

A5131 Define IA Strategies, Policies, and Plans: This activity establishes current and future IA goals, objectives, and implementing plans and procedures, and assigns roles and responsibilities for all IA modernization, operations, sustainment, and readiness including IA portfolio investment management. Outputs of this activity provide the EIEMA oversight authorities the basis for measuring IA-related activity performance at all levels of the enterprise.

A5132 Define Systems and Network Management Strategies, Policies, and Plans: This activity establishes current and future systems and networks goals, objectives, and implementing plans

and procedures, and assigns roles and responsibilities for all systems and networks modernization, operations, and sustainment including systems and networks portfolio investment management. Outputs of this activity provide the EIEMA oversight authorities the basis for measuring systems and networks related activity performance at all levels of the enterprise.

A5133 Define Content Staging Strategies, Policies, and Plans: This activity establishes current and future content-staging goals, objectives, and implementing plans and procedures, and assigns roles and responsibilities for content-staging infrastructure, operations, sustainment, and readiness. Outputs of this activity provide the EIEMA oversight authorities the basis for measuring content-staging related activity performance at all levels of the enterprise.

A514 Develop Net-Centric Data Strategies, Policies, and Plans: This activity involves the development of data strategies, policies and plans that codify the tenants of the Net-Centric Data Strategy. Specifically, this activity describes the activities that should be conducted to determine: what data assets are available, how will those assets be shared, how the community will enforce data sharing and how new/existing architectures should be created/updated to implement the Net-Centric Data Strategy.

A5141 Develop Net-Centric Data Asset Management Plan: This activity involves inventorying data assets and prioritizing the data assets that should be published to the Enterprise. This activity should be conducted on a regular basis to ensure that newly developed data assets are prioritized in relationship to existing data assets and that resources are leveraged to ensure that data assets of the highest value are made visible and accessible to the Enterprise at the earliest possible time in its data lifecycle.

A51411 Develop Data Asset Publication Policies: This activity involves identifying appropriate formats and publication options to ensure that visible and accessible data assets are useable by the widest community of users. Every effort should be made to ensure that data assets published to the Enterprise utilize these specifications and support the enterprise data asset publication specification.

A51412 Identify Data Assets: This activity calls for data owners, data producers, information management staff, and others to determine what data assets (documents, images, metadata, services, etc) are produced or controlled within a community. This information is compiled and maintained in a data asset listing which should be updated regularly to ensure that newly developed and newly retired data assets are tracked accordingly.

A51413 Prioritize Data Assets: This activity involves evaluating the data asset listing to determine which assets have the highest value to the Enterprise, and determine a data asset prioritization methodology. This methodology should be maintained as part of regular planning processes. Prioritization of data assets can be accomplished using a variety of criteria (e.g. highest value to expected users, usage frequency, etc.) as determined at the discretion of the community.

A51414 Define Authoritative Sources: This activity involves reviewing the prioritized data asset listing and identifying authoritative sources of data within the community. These authoritative sources should be incorporated into the business processes used within the community by its applications and systems and visible to enterprise users.

A5142 Develop Net-Centric Data Asset Sharing Plan: The activity involves the development of comprehensive net-centric plans to facilitate the sharing of identified data assets. Fundamental to this activity is the determination of how to tag data assets and the infrastructure required to support sharing of these assets with the Enterprise.

A51421 Develop Data Asset Tagging Plan: This activity details the steps needed to create a data asset tagging plan. This plan outlines the approach for providing semantic and structural information about data assets within a community. Data Asset Tagging plans should utilize the Net-Centric Data Asset Management Plan to tailor tagging of Data Assets based on the key types of data assets managed by the community. This plan should address: 1) The type of information that should be associated with each data asset, 2) How tags should be provided/bound to data assets, 3) Identification of required policies required, 4) Identification of

metrics and tagging incentives, 5) Plan for incorporation of tagging into community tools and capabilities and doctrine.

A514211 Develop Data Asset Tagging Guidelines: Communities should develop recommended tagging guidelines to define rules and circumstances when tagging is appropriate, identify tagging levels (e.g. record-level, asset-level, inline.), and methodologies for tagging data assets (e.g. automated, manual, portal based).

A514212 Develop COI-Specific Discovery Metadata Specifications: This activity involves extending the DoD Discovery Metadata Specification (DDMS) with community specific elements. These additional information elements enhance a communities ability to describe data assets and support their specific mission objectives (e.g. A community could extend the DDMS with the field 'unit code' to identify the exact unit that a data asset originated.). Community DDMS extensions should be registered in an enterprise accessible Metadata Registry.

A51422Develop Data Infrastructure Plan: This activity involves the development of plans for Communities to implement/utilize the infrastructure items of the Net-Centric Data Strategy. Deploying a Net-Centric Data Infrastructure requires resources for both deployment and long-term maintenance. Therefore, communities should utilize existing data infrastructure whenever possible to minimize this impact (e.g. provided by its associated Domain(s)). Where existing data infrastructure is being utilized by a community, the Data Infrastructure Plan should detail the plans for utilizing this infrastructure (e.g. service level agreements, etc.).

A514221 Develop Discovery Catalog Plan: This activity develops a plan for the implementation/utilization of Discovery Catalogs. Discovery Catalogs contain DDMS compliant "metacards" describing data assets contained within a community. The Discovery Catalog plan should provide sufficient detail to support the development/management of discovery catalogs, discoverability of data assets, implementation/management of the enterprise discovery interface specification, DoD-Wide Enterprise federation, plan for supporting the DDMS and development of needed policies/procedures to support the catalog. Discovery catalogs can be implemented/utilized in a multitude of ways; therefore, each community should develop plans that work best for their environment.

A514222 Develop Metadata Registry Plan: This activity develops a plan for the implementation/utilization of a Metadata Registry. Metadata management is an important activity in implementing a successful net-centric data strategy. Metadata Registries provide a means to store and manage structural and definitional metadata assets. Metadata Registries can be useful in supporting convergence of metadata standards and to manage common models across communities. Metadata stored in metadata registries are typically utilized by developers, business analysts, and architects. The Metadata Registry plan should provide sufficient detail to support the development/management of metadata registries, discoverability of metadata assets, implementation/management of the enterprise discovery interface specification, enterprise federation, a plan for supporting the DDMS and development of needed policies/procedures to support the registry. Metadata Registries can be implemented/utilized in a multitude of ways; therefore, each community should develop plans that work best for their environment. Communities are encouraged to utilize the DoD Metadata Registry; however, if a community does set up their own metadata registry, they must ensure that metadata assets are visible by the DoD Metadata Registry. The DoD Metadata Registry can be found at http://metadata.dod.mil.

A514223 Develop Services Directory Plan: This activity develops a plan for the implementation/utilization of a Services Directory. Services Directories are a key component of a service oriented architecture as they enable communities to discover and use services that have been published. The Services Directory plan should provide sufficient detail to support the development/management of Services Directories), discoverability of services, implementation/management of the Discovery Interface Specification, DoD-Wide Enterprise federation and development of needed policies/procedures to support the Services Directory.

Service Directories can be implemented/utilized in a multitude of ways; therefore, each community should develop plans that work best for their environment.

A514224 Develop COI Directory Plan: This activity develops a plan for the implementation/utilization of a Community of Interest (COI) Directory. COI Directories provide a location to register and describe COI that have been established within the Department of Defense. Registering a COI enables Communities throughout the DoD to discover and contact Communities that support their specific mission. The COI Directory plan should provide sufficient detail to support the development/management of COI Directories, discoverability of COI(s), implementation/management of the enterprise discovery interface specification, enterprise federation and development of needed policies/procedures to support the COI Directory. COI Directories can be implemented/utilized in a multitude of ways; therefore, each community should develop plans that work best for their environment.

A514225 Develop Enterprise Discovery Federation Plan: This activity develops an Enterprise Discovery Federation plan to address federating catalogs, registries, and directories with the Enterprise Discovery service.

A514226 Integrate Data Infrastructure Plans: This activity compiles the Discovery Catalog, Metadata Registry, Services Directory, COI Directory and Enterprise Discovery Federation plans into a cohesive Data Infrastructure Plan.

A5143 Develop Net-Centric Data Guidance: This activity evaluates the information from sources such as compliance reports, incentive plan reports, policy, and user needs to create net-centric data guidance. Data guidance is the policy, specifications, standards, etc., used to drive data activities within the Community. It differs from a Net-Centric Data Asset Sharing Plan in that it is more strategic in nature. Data guidance may be a subset of an overall net-centric data sharing plan.

A51431 Define Data Metrics/Incentives: This activity establishes the basis for measuring and encouraging progress in implementing the Net-Centric Data Strategy. Defined metrics are used to track the progress made towards establishing a net-centric data environment within a Community. Examples of data metrics include percent of web-enabled components, progress toward service-enabling identified key functional components and percent of tagged Community data. Incentives should be developed and provided to the pertinent Communities to encourage participation in the net-centric data activities.

A51432 Define Net-Centric Data Strategies: This activity includes the identification of data goals and overarching vision for each Community. Once identified, the data strategy should include objectives and activities that outline how to accomplish the goals of establishing a net-centric data environment. Data strategy documents should be well vetted within the Community to ensure it outlines a vision that meets the needs of its stakeholders and should precede or accompany formal policy.

A51433 Define Net-Centric Data Policies: This activity utilizes the strategies previously defined to develop policies for establishing a net-centric data environment. Net-Centric Data Policies are important for institutionalizing the Net-Centric Data Strategy within a Community.

A52 Develop Enterprise Information Environment Capabilities: This activity consists of the design, planning and engineering, and implementation of the DoD net-centric information environment's initial and incremental capabilities. It takes system and network functional and operational performance requirements as inputs and produces capability designs, plans, implemented capabilities and their controlled incremental integration and activation. This activity is controlled by the operational environment; plans; policies; guidance; laws and regulations; tactics, techniques, and procedures; standards; and funding. It is enabled by Global Information Grid (GIG) systems and networks; net-centric enterprise services; net-centric Community of Interest (COI) applications and services; GIG NetOps facilities; GIG NetOps personnel; Service CIOs, PEOs, Acquisition Executives, Program Managers, etc.

A521 Architect Enterprise Information Environment Service Capabilities: This activity aggregates the functions of developing operational, system, and technical architecture products for the

purpose of specifying and implementing new or modified capabilities within the information environment. This activity takes capability improvement opportunities and needs as inputs and produces net-centric information environment architectures, Community of Interest (COI) data models and environment standards as outputs. Capabilities addressed must include both physical and technical security.

A5211 Architect Net-Centric Core Enterprise Capabilities: This activity provides the architectural products for core enterprise capabilities (e.g., Net-Centric Core Enterprise Services [NCES]). These products are used to articulate, analyze, control, and implement new or modified core capabilities within the net-centric information environment.

A5212 Architect Community of Interest Capabilities: This activity provides the architectural products for each functional or cross-functional Community of Interest (COI) that is supported within the information environment. These products are used to articulate, analyze, control, and implement new or modified COI capabilities within the net-centric information environment.

A5213 Architect Enterprise Net-Centric Data Capabilities: This activity creates and builds upon existing and revised architectures and plans to support information sharing objectives. The architecture should depict components that emphasize the discovery, services-based approach to systems engineering, metadata use to support mediated information exchange and web-based access to data assets.

A5214 Architect Net-Centric Enterprise Control Services: This activity provides the architectural products for enterprise control services (e.g., information assurance controls, network service controls, and content staging controls) that must be available to properly operate the EIE in compliance with established policies. These services must be used within the EIE to make policy enforcement decisions and to provide policy enforcement execution.

A5215 Manage Information Environment Standards: This activity aggregates the functions of developing, evaluating, selecting, and applying the set of standards that are essential to the effective and efficient implementation of the information environment. This activity may be initiated as a result of emerging technology, activities of commercial standards bodies or consortia, or a recognized need to reduce the variety of standards being used within the information environment. This activity produces inputs to evolving standards and maintains the Joint Technical Architecture and its associated products.

A522 Plan and Engineer Information Environment Capability Increments: This activity aggregates the functions of extending and evolving the capabilities of the information environment. It pertains to implementing required system and network capabilities, information management, and applications for a mission or for an incremental improvement in the information environment. It focuses on defining, establishing, evolving, and integrating the information environment computing and communications functionality in response to operational (mission) requirements, and designing in security. It includes the planning and engineering of NetOps support capabilities. This activity receives a capability extension need from the information environment as an input and produces capability increment implementation and funding plans as well as capability incremental designs as outputs. Environment architectures, institutional Community of Interest (COI) data models and environment standards taken from the design of the information environment capabilities control this activity. Capabilities addressed must include both physical and technical security.

A5221 Plan and Engineer System Capabilities: This activity focuses on the functions of extending and evolving the Global Information Grid (GIG) computational infrastructure. It includes defining, establishing, evolving, and integrating GIG computing functions in response to operational (mission) requirements. It pertains to computing hardware and operational databases.

A52211Plan and Engineer Computer Hardware and Software Installation: This activity focuses on the specific computer hardware and associated software to be installed and integrated into the Global Information Grid (GIG) as part of a new and/or evolving functional capability. NetOps personnel perform this activity. The inputs to this activity are GIG architecture information,

physical plant constraints, and computer and software resources. It provides installed computational capabilities that can support operational needs. Such engineering may include the design of anti-tamper and radiation hardened devices. DoD policy, guidance, funding, GIG architectural governance, functional performance requirements, and engineering best practices provide controls to this activity.

A52212 Coordinate System Capability Planning and Engineering with Commercial Provider: This activity focuses on the process of gaining service-level agreements, standard net-centric operating procedures, and functional performance capabilities from computing operations that have been outsourced to a Commercial Provider (e.g., Navy Marine Corps Intranet [NMCI]). It addresses the specific computer hardware and associated software to be installed and integrated into the Global Information Grid (GIG) as part of a new and/or evolving functional capability. It includes defining, establishing, evolving, and integrating GIG computing functions in response to operational (mission) requirements. Commercial Provider and DoD NetOps personnel perform this activity. The inputs to this activity are GIG architecture information, physical plant constraints, and computer and software resources. It provides new service level agreements, updates to standard net-centric operating procedures, and installed computational capabilities that can support operational needs. DoD policy, guidance, funding, contracts, GIG architectural governance, functional performance requirements, and engineering best practices provide controls to this activity.

A52213 Define Administrative Domains, Authorities, and Responsibilities: This activity focuses on establishing the administrative boundaries within the Global Information Grid (GIG), identifying authorities to oversee and control actions within these boundaries, and assigning specific responsibilities to NetOps personnel within these boundaries as well as cross-domain responsibilities and authorities.

A52214 Plan and Engineer System Software: This activity focuses on selecting, sizing, and loading those applications that operate the Global Information Grid (GIG) infrastructure or are used to administer the GIG infrastructure (e.g., Operating Systems, System Utilities, Data Management Systems, Auditing Software, and System Management and Reporting Applications, Monitoring Software). NetOps personnel perform this activity. It takes hardware configurations, GIG architecture information, and Standard Net-Centric Operating Procedures, and supplies system applications that run and manage the GIG. The planning and engineering are constrained by hardware configurations, standard NetOps (Net-Centric) operating procedures, and the quantity of domains being supported.

A52215 Coordinate Establishing Content and Content Mapping: This activity focuses on loading content and mapping that content at system initialization/re-initialization. It is coordinated by NetOps Content Managers and performed by NetOps Administrators. It is controlled by the functions to be performed within the extended elements of the Global Information Grid (GIG), the storage resources available, and by standard Net-Centric operating procedures.

A52216 Plan and Engineer Systems Management and Reporting Systems: This activity focuses on establishing the system management and reporting responsibilities and capabilities for each new Global Information Grid (GIG) extension or evolution. It is performed by NetOps personnel and implemented by NetOps administrators. It takes policy, guidance, GIG NetOps management structures, and standard Net-Centric operating procedures as controls. It produces new or revised integrated operational management and reporting capabilities for the GIG.

A5222 Plan and Engineer Network Capabilities: This activity focuses on the functions of extending and evolving the Global Information Grid (GIG) networking infrastructure. It includes defining, establishing, evolving, and integrating GIG networking functions in response to operational (mission) requirements. It pertains to network hardware, network media modes, and network facilities.

A52221 Plan and Engineer Transmission and Switching Systems: This activity focuses on providing new Local and Wide Area information transport capabilities through the engineering of new

bandwidth, physical wiring, router topologies, and switching capabilities, wireless transmission cells, gateways and Public Switched Telephone Network (PSTN) isolation, etc. It takes desired information transport capabilities as input. It is controlled by policy, guidance, networking "best practices," existing resources (including commercial provisioning capabilities), connectivity requirements, environmental constraints, and optimizing of information flows. It produces new or evolved integrated extensions to the Global Information Grid (GIG) information transport capabilities. NetOps Communications Engineers perform this activity.

A52222Coordinate Network Capability Planning and Engineering with Commercial Provider: This activity focuses on the process of gaining communications service-level agreements, standard net-centric operating procedures, and functional performance capabilities from networking operations that are to be provisioned by a Commercial Provider. This networking capability may be provisioned in the form of information transport over host-nation commercial facilities or through transport provisioned by a U.S. commercial provider. It is usually implemented through contractual arrangements or a service level agreement. It addresses the specific connections, transmission media, networking hardware and associated software to be installed and integrated into the Global Information Grid (GIG) as part of a new and/or evolving information transport capability. It includes defining, establishing, evolving, and integrating GIG networking functions in response to operational (mission) requirements. Commercial Provider and DoD NetOps personnel perform this activity. This activity may use auction services to fill peak demands in a more dynamic fashion. The inputs to this activity are GIG architecture information, desired networking operational capabilities, physical plant constraints, and computer and software resources. It provides new contracts, service-level agreements, updates to standard net-centric operating procedures, and installed information transport capabilities that can support operational needs. DoD policy, guidance, funding, contracts, GIG architectural governance, functional performance requirements, and communications engineering "best practices" provide controls to this activity.

A52223Define Network Demarcations, Authorities and Responsibilities: This activity establishes the boundaries of Global Information Grid (GIG) networks, gateways through which information import/export must occur and where external users must enter into GIG networks. The activity assigns network responsibilities and identifies authorities for executing oversight and control of assigned network responsibilities. Network demarcations may be established within the GIG to provide additional controls.

A52224Plan and Execute Electromagnetic Frequency Assignments: This activity generates frequency assignments-an authorization for use of a specified range of the electromagnetic spectrum, at a specified location, with specified equipment, for a specified purpose, by a specified organization. Generation of frequency assignments takes into account capabilities of the spectrum-using equipment, prevention of harmful interference to other spectrum-using equipment, and any operational restrictions on frequencies available for use. "Permanent frequency assignments" are coordinated with host-nation spectrum management activities. Tactical frequency assignments address the day-to-day employment of the electromagnetic spectrum within the authorized permanent frequency assignments.

A52225Plan and Engineer Network Management and Reporting Systems: This activity focuses on establishing the network management and reporting responsibilities and capabilities for each new Global Information Grid (GIG) extension or evolution. It is performed by NetOps personnel and implemented by NetOps administrators. It takes policy, guidance, GIG NetOps management structures, and standard Net-centric operating procedures as controls. It produces new or revised integrated operational management and reporting capabilities for the GIG.

A52226Coordinate Tactical Reach-back: This activity coordinates the establishment of extensions of the Global Information Grid (GIG) communications backbone to tactical forces. It coordinates the establishment of Theater Injection Points and in coordinating and consolidating Theater broadcast schedules. NetOps personnel at Global, Theater, and Joint Force Command,

Control, Communications and Computers (C4) Coordination Centers, and at Standard Theater Teleport Sites perform this coordination activity with various Network Operations and Security Centers (NOSCs) and System Controllers (SYSCONs). The inputs to this activity are the request to establish a Theater Injection Point, Reach-back connectivity requirements, and Tactical Broadcast Scheduling Requirements. The output of this activity is operations extensions of GIG connectivity to tactical forces, reach-back connectivity, and updated Tactical Broadcast Schedules.

A5223 Plan and Engineer NetOps Support Capabilities: This activity focuses on the functions of extending and evolving the Global Information Grid (GIG) infrastructure management, operations management, and protection capabilities. It includes defining, establishing, evolving, and integrating GIG NetOps functions in response to operational (mission) requirements. It pertains to the GIG Trust Infrastructure, protection mechanisms, sensor mechanisms, network management systems (e.g., Simple Network Management Protocol (SNMP)-based management), Network Facilities Management, Information Dissemination Management Systems (e.g., Global Broadcast System), and Net-Centric Core Enterprise Services Infrastructure

A52231Plan and Engineer Integrated NetOps Monitoring and Response Capabilities: This activity focuses on establishing integrated NetOps management and reporting responsibilities and capabilities for each new Global Information Grid (GIG) extension or evolution. It is performed by NetOps personnel and implemented by NetOps administrators. It takes policy, guidance, GIG NetOps management structures, and standard Net-centric operating procedures as controls. It produces new or revised integrated operational management and reporting capabilities for the NetOps personnel managing the GIG.

A52232Plan and Engineer Integrated NetOps Management Capabilities: This activity focuses on the functions of extending and evolving the Global Information Grid (GIG) infrastructure management, operations management, and protection capabilities. It includes defining, establishing, evolving, and integrating GIG NetOps functions in response to operational (mission) requirements. It includes the assignment of responsibilities and the identification of authorities for integrating management of newly extended or evolving GIG infrastructure. It is coordinated by NetOps personnel and implemented by NetOps administrators.

A52233Define Status Reporting Requirements: This activity focuses on the reporting requirements at various levels of NetOps management to ensure NetOps personnel can maintain Global Information Grid (GIG) situational awareness. Situational-awareness requirements, policy, guidance, monitoring capabilities, and standard NetOps operating procedures control this activity. NetOps personnel perform this activity. This activity takes desired situational awareness capabilities as inputs, and produces standardized NetOps status reporting procedures, an established reporting hierarchy, and identified authorities for overseeing and controlling NetOps reporting as outputs.

A52234Plan System and Network Logistics: This activity addresses coordinating logistics aspects (e.g., electrical power, contracted corrective- and preventative-maintenance, spare parts, storage media, air-conditioning, air-filtering, repair facilities, storage facilities, and facilities management including logistics in support of Force Protection Measures). This activity is performed by local-facility NetOps personnel and is coordinated through Command, Control, Communications and Computers (C4) Coordination Centers. It takes as inputs NetOps logistics needs and provides NetOps logistics provisioning plan(s). It is controlled by policy, guidance, standard NetOps operating procedures, and logistics management standards.

A523 Implement Information Environment Increments: This activity consists of the actual implementation of a specified capability increment. It includes the acquisition, integration, and activation of a capability increment. This activity produces information environment capabilities. This activity is controlled by current implemented capabilities and funding plans and incremental capability designs. Capability increments must implement both physical and technical security as previously planned and engineered.

A5231 Acquire Capability Increment: This activity provides the various means to acquire increments of capability for the Enterprise Information Environment. It consists of sub-activities that involve Service/Joint acquisition development programs, Agency procurement programs, and contracted foreign/domestic commercial capabilities.

A5232 Integrate Capability Increment: This activity provides the various means to integrate new increments of capability into the existing information environment. The process takes the new increment and composes it with the existing enterprise information environment to yield a modified environment. It requires identifying the elements to be fully integrated (i.e., their independent elements become hidden in composition) and those to be interfaced (i.e., the coupling together of less-compatible increment elements with connectors and adaptors at their interfaces). Integration may include eliminating some legacy elements to enable composition of the remaining legacy elements with the new capability increment elements. The testing and analysis of the integrated result is performed within sub-activities of A56. Integration uses the sub-activities of A52 to manage the configuration of this integration process.

A5233 Activate Capability Increment: This activity provides the actual turnover of capabilities newly integrated within the information environment to the operators and to the environment managers. It accepts the output of A56 (e.g., certification for operations) and provides the accreditation authority's "approval to operate."

A53 Manage EIE Infrastructure Capabilities and Operations: These activities involve the actions required to effectively and efficiently manage the capabilities and operations associated with the infrastructure.

A531 Manage Services: This activity focuses on establishing and maintaining the various services in the EIE. These enterprise services, in conjunction with automated applications, provide the means required by the user community to capture and leverage user knowledge and experience. These services make information and applications accessible across the information environment and provide users the means to take full advantage of the capabilities of the environment. This activity is performed by NetOps Administrators. The activity takes various common service resource needs as input and produces appropriate service functionality as output. It is controlled by policy and guidance. It is enabled by Global Information Grid (GIG) systems and networks; net-centric enterprise services; net-centric Community of Interest (COI) applications and services; GIG NetOps facilities; and GIG NetOps personnel.

A5311 Manage Core Services: This activity involves the management of all aspects of the core enterprise services.

A53111 Manage User Agent Services: This activity involves the management of all services associated with the User Agent.

A53112 Manage Discovery Services: This activity involves the management of all services associated with Discovery.

A53113 Manage Collaboration Services: This activity focuses on the maintenance and control of the services necessary to establish, maintain, and dissolve specific collaborations. It supports the negotiated configuration, activation, and integration of individual collaborative sessions. This includes connectivity resources, shared audio visualization and production resources, and communications support. The activity supports a user's ability to interactively participate in a collaboration. This support can include the physical connection to the virtual workspace; enabling the viewing and manipulating information in a common forum; providing a shared workspace, whiteboard, shared applications, capabilities for interactive analysis of information, and interactive development and editing of documents/briefings. This activity takes as input a submitted set of requirements for collaboration, including specified participants, classification, purpose, schedule, duration, and specific collaborative tools needed. It produces as output the allocation of resources and the controls necessary to conduct that collaboration.

A53114 Manage Messaging Services: This activity consists of all activities needed to support formal (organizational and/or structured) and informal (email and/or unstructured) messaging services. It includes support for tactical requirements. It supports the composition and validation

of outgoing messages (message preparation). It supports the processing of incoming messages, including subsequent distribution to intended recipients as users of the information environment. The activity establishes and conducts message (bulletin) board services. It also supports official message traffic.

A531141 Manage Message Boards: This activity focuses on the establishment and maintenance of both moderated and un-moderated message boards based on requests for the establishment of a message board, message board profiles, and rule sets.

A531142 Manage Tactical Data Links: This activity focuses on the establishment and maintenance of specified tactical data links based on tactical participants, operational requirements, and dynamics of the situation.

A531143 Manage Email; This activity focuses on the establishment and maintenance of email capabilities based on operational requirements.

A531144 Manage Record Traffic: This activity focuses on the establishment and maintenance of official message traffic based on policy, doctrine, and operational context. The activity ensures that established record traffic priorities and protection measures are followed. It also ensures that plain language addresses are maintained to support record traffic dissemination.

A53115 Manage Mediation Services: This activity involves the management of all services associated with Mediation.

A53116 Manage Storage Services: This activity manages the distributed environment that serves as the information environment repositories. These include major index maintenance, enabling of information storing, retrieving, and archiving. Manages the persistent stores of data to ensure consistent availability, accessibility, reliability and persistence. Backs up information for future use or to support recovery activities. This management activity focuses on the efficient use of storage and its relationship to overall system and network performance. It analyzes and integrates content placement requirements based on operational needs and current performance assessments. It provides a set of prioritized, integrated requirements for relocating or re-staging content. It is controlled by policy, resource and information management guidance, and content staging procedures established by NetOps content managers. NetOps administrators perform this activity.

A531161 Manage Content Placement: This activity focuses on the dynamic aspects of achieving efficient content-access, effective information protection, and optimizing overall performance within the information environment. This activity involves designing restaging approaches, assessing restaging feasibility, and executing restaging operations. It supports load balancing by moving content, replicating content, and locating content for specific operations (e.g., broadcast consolidation). It supports export of information from the information environment. It may be used to reduce the value of a target site or to take advantage of protections afforded within different storage locations. It may require re-mapping of directories, catalogs, etc. It is coordinated by NetOps Content Managers (e.g., Command Information Management Officers) and performed by NetOps Administrators. It takes dynamic performance measures and operational requirements (e.g., user demands) as input, and produces new content locations and mappings. It is controlled by policy and operational guidance.

A531162 Manage Databases: This activity focuses on the establishment and lifecycle maintenance of various forms of databases (e.g., relational, object-based). Users, Community of Interest Management, and NetOps administrators manage databases schemas and content appropriate to their needs. NetOps administrators coordinate and manage the resources upon which these databases reside.

A531163 Manage Portals: This activity focuses on the design, maintenance, and control of portals. Community of Interest (COI) Managers and NetOps administrators manage these portals by providing the specific procedures, rules, and requirements for placing content and/or content references on a portal. NetOps administrators, specifically assigned, are responsible for conducting the OPSEC review of material placed on a portal.

A53117 Manage Application Services: This activity involves the management of all services associated with Application development.

A5312 Manage COI Services; This activity enables the performance of all actions associated with the administration of services provided by the Community of Interest (COI). The services available to an individual user may be altered from those specified in a user role.

A5313 Manage Environment Control Services: This activity involves the management of all aspects of the environment control services.

A5314 Manage User-Profile Services: This activity provides administrative services for user modification, automatic update, or mission-driven changes to profile data. The user profile contains significant features for the user's information requirements based on role, responsibilities, and work objectives. This activity includes those actions individual users take to define, maintain, and activate their dynamic profile requirements, criteria, and attributes. For example:1) The requirements define what information the user desires access to (e.g., a need for mapping data). The criteria define the user-desired threshold for information (e.g., a mapping requirement is for 1:50,000 scale or larger within EUCOM) 2) The basic attributes of the user's profile are determined by the organization to which the user belongs and the user's role in that organization. Example attributes include user roles, Community of Interest (COI) membership, areas of responsibility, clearances, accesses, and communications medium. Profile activation includes submitting the profile to the information environment for storage and use. These administrative services implement a combination of human and automated means to review, verify, and validate both the user and provider-specified portions of the dynamic profile. In establishing the profile, the user makes all information within the profile available for use. The dynamic profile is used in connection with ad hoc queries to refine search specifications and is also used with intelligent agents to automatically identify and deliver relevant information to the user.

A53141 Identify Administrator-Defined Elements of User Profile: This activity identifies the administrative requirements and defines system-level requirements for managing user profile resources. The user requirements specify what information the user desires access to (e.g., a need for mapping data) as well as related selection criteria (e.g., 1:50,000 scale or larger for EUCOM). The administrator requirements specify what system-level information must be statically placed into the user profile (e.g., identity information), and what information must be dynamically placed into or bound to the user profile (e.g., active role, current active group association, user-assistant modifiable information).

A53142 Perform User Profile Administration: This activity provides profile parameters, links, and/or profile-enabling program binding for a user profile to make the profile executable.

A5315 Manage Restoration Services; This activity focuses on monitoring the information environment and the activation of restoration activities as needed. It takes as input information environment events and resource status, produces activated restoration activities as outputs. The activity is controlled by rule sets.

A532 Manage Communities of Interest: This activity involves the establishment of Communities of Interest (COI) and corresponding COI specific activities. Communities of Interest (COIs) are an appropriate construct for defining information exchange formats and metadata definitions as well as vocabularies used to communicate within the COI.   Therefore, once established, COIs should leverage the data strategy activities identified elsewhere in the NCOW model to support the goals of the Net-Centric Data Strategy (e.g. Ensure Data Asset Understandability, Provide Data Assets, etc.).

A5321 Identify COIs: This activity identifies appropriate groups of people who should come together to support common mission objectives. Communities will form in a variety of ways and may be composed of members from one or more functions and organizations as needed to support mission needs.

A5322 Establish Communities of Interest: This activity involves establishing Communities of Interest and ensuring their visibility to the Enterprise. At a minimum, COIs should develop a

charter and identify the governance structure needed to support their Community. Once established, COIs should register in a federated COI Directory to enable DoD users to discover groups which are performing activities of interest.

A53221Develop Community of Interest Charter: This activity describes a Community of Interest's mission, roles, responsibilities and objectives into a formal COI Charter. This charter can then be registered in the COI Directory to facilitate understanding of a COI's focus for users DoD-wide.

A53222Identify COI Governance: This activity involves the identification of governance bodies/constructs that support the mission of a COI.

A53223Register in COI Directory: This activity involves providing DDMS compliant metadata about a Community of Interest (COI) to a federated COI Directory. Every Community of Interest (COI) should register itself into a federated COI Directory. This COI Directory should allow COIs to register their existence, points of contact, membership, mission/charter, and provide future COI collaboration capabilities. Providing this information facilitates the Net-Centric Data Strategy goals of visibility and understandability by ensuring that users on the Global Information Grid can locate and contact Communities with missions of interest.

A5323 Manage Feedback Mechanisms: This activity supports goal to increase the integrity and quality of visible data in the Department of Defense. Communities should identify and establish processes to evaluate/refine the user experience and quality of data assets (e.g. ratings for data access mechanisms, data assets, metadata usability, etc.). Additionally, these feedback mechanisms allow COIs to identify previously unanticipated users and applications.

A5324 Manage Community of Interest Membership: This activity enables the performance of all actions associated with membership administration in a Community of Interest (COI). This includes adding or deleting users from a COI, or changing user profiles and user roles, as appropriate.

A53241Manage User Roles: This activity enables the performance of all actions associated with user role administration within the Community of Interest (COI). The user role defines the sub-COIs the user belongs to, the user's subscriptions to catalog products, and the services available to members of the COI.

A53242Manage Community of Interest Profile: This activity provides administrative services for COI modification, automatic update, or mission-driven changes to profile data. The COI profile contains significant features for the COI's information requirements based on role, responsibilities, and work objectives. This activity includes those actions individual COIs take to define, maintain, and activate their dynamic profile requirements, criteria, and attributes. These administrative services implement a combination of human and automated means to review, verify, and validate portions of the dynamic profile. In establishing the profile, the COI makes all information within the profile available for use. The dynamic profile is used in connection with ad hoc queries to refine search specifications and is also used with intelligent agents to automatically identify and deliver relevant information to the user.

A5325 Manage Community of Interest Subscription: This activity enables the administration of both the Community of Interest (COI) subscription to external products, and members' subscriptions to internal products. An individual's subscriptions can be altered from those specified in a user role.

A533   Manage Data Infrastructure: This activity pertains to the establishment and management of components of the Net-Centric Data Infrastructure. In these activities, software/hardware solutions are implemented and maintained. Additionally, the infrastructure activities include the development of metadata products that support information exchange (e.g. they are the foundation for instance documents and drive run-time interoperability).

A5331 Manage Discovery Catalogs: This activity involves the establishment and management of discovery catalog components. In this activity discovery catalog structure is defined and discovery catalog infrastructure (hardware/software) is implemented and maintained. This activity also includes the configuration management and maintenance of the Discovery Interface Specification and corresponding DDMS updates. Implementations will vary, and

physically storing metadata information in a catalog is not required. Rather, any method can be used to provide "cataloging-like" capabilities such as dynamic indexed searches and interrogative searching.

A53311Determine Discovery Catalog Structure: This activity focuses on defining the structure of how data assets will be organized within the discovery catalog(s). This structure should utilize the ontologies developed under "Ensure Data Asset Understandability".

A53312Establish Discovery Catalogs: This activity focuses on identifying and/or establishing physical discovery catalogs for managing tagged data assets and supporting Enterprise-wide discovery.

A53313Maintain Discovery Catalogs: This activity involves ensuring the physical, software and data contained within a Discovery Catalog is maintained. It includes functional revisions to infrastructure software/hardware, maintaining the Enterprise Discover Interface, managing changes to the DDMS, ensuring cataloged data assets contain up-to-date information and are accessible from their specified locations.

A5332 Manage Service Directories: NThis activity involves the establishment and management of service directory components. In this activity service directory structure is defined and infrastructure (hardware/software) is implemented and maintained. This activity also includes the configuration management and maintenance of the Discovery Interface Specification and corresponding DDMS updates.

A53321Determine Service Directory Structure: This activity focuses on defining the structure of how services will be organized within the Services Directory. This structure should utilize the ontologies developed under "Ensure Data Asset Understandability".

A53322Establish Service Directories: This activity identifies and/or establishes physical service directories for managing registered services and supporting Enterprise-wide discovery.

A53323Maintain Service Directories: This activity involves ensuring the physical, software and data contained within a Service Directory is maintained. It includes functional revisions to infrastructure software/hardware, maintaining the Enterprise Discover Interface, managing changes to the DDMS and ensuring cataloged services contain up-to-date information.

A5333 Manage COI Directories: This activity involves the establishment and management of COI directory components. In this activity COI directory structure is defined and infrastructure (hardware/software) is implemented and maintained. This activity also includes the configuration management and maintenance of the Discovery Interface Specification and corresponding DDMS updates.

A53331Determine COI Directory Structure: This activity focuses on defining the structure of how COI(s) will be organized within the COI Directory. This structure should utilize the ontologies developed under "Ensure Data Asset Understandability".

A53332Establish COI Directories: This activity identifies and/or establishes physical COI directories for managing registered COI(s) and supporting Enterprise-wide discovery.

A53333Maintain COI Directories: This activity involves ensuring the physical, software and data contained within a COI Directory is maintained. It includes functional revisions to infrastructure software/hardware, maintaining the Enterprise Discover Interface, managing changes to the DDMS and ensuring cataloged COI(s) contain up-to-date information.

A5334 Ensure Data Asset Understandability: This activity focuses on ensuring that users and applications can comprehend data assets, both structurally and semantically. Semantic understanding is achieved through the use of ontologies that reflect a Communities understanding of their shared data. Structural understanding is achieved by registering structural metadata artifacts to the DoD Metadata Registries that enable developers, business analysts and architects to review the structure of a data asset.

A53341Manage Metadata Registries: This activity involves the establishment and management of metadata registry components. In this activity metadata registry structure is defined and infrastructure (hardware/software) is implemented and maintained. This activity also includes

the configuration management and maintenance of the Discovery Interface Specification and corresponding DDMS updates.

A533411 Determine Metadata Registry Structure: This activity focuses on defining the structure of how metadata artifacts will be organized within the Metadata Registries. This structure should utilize the ontologies developed under "Ensure Data Asset Understandability".

A533412 Establish Metadata Registries: This activity of identifies and/or establishes physical metadata registries for managing metadata artifacts and supporting Enterprise-wide discovery.

A533413 Maintain Metadata Registries: This activity involves ensuring the physical, software and data contained within a Metadata Registry is maintained. It includes functional revisions to infrastructure software/hardware, maintaining the Enterprise Discover Interface, managing changes to the DDMS and ensuring cataloged metadata artifacts contain up-to-date information.

A53342 Define Ontologies: The activity involves the development ontologies that reflect a Communities understanding of their shared data. Ontologies promote semantic and syntactic understanding of data (e.g. taxonomies enhance discovery by providing a hierarchical means of searching for data while providing users with additional insights about data assets by indicating their placement relative to other data assets). Ontologies include taxonomies, thesauri, vocabularies, and associations.

A533421 Define Vocabularies: This activity involves identifying and defining terms and their respective definitions. This vocabulary can then be used for defining a Community's taxonomy or metadata keyword listing. Developed vocabularies help to insure that metadata is identified using unambiguous, non-redundant terms.

A533422 Define Taxonomies: This activity involves the development or identification of a classification scheme that relates one vocabulary term to another, and is used to map vocabulary elements and assertions among them.

A533423 Define Ontology Relationships: This activity determines the semantic relationships between terms in a vocabulary to facilitate expansion of search and understanding capabilities. This activity involves defining a many-to-many relationship of assertions between terms in the vocabulary. This activity is typically second-order to initial search capabilities.

A533424 Ensure Ontology Visibility: This activity involves posting of ontology data to a Federated Metadata Registry. Publishing ontology information to a Metadata Registry facilitates understanding across the enterprise.

A5335 Manage Interoperability Components: This activity involves the identification, development, and maintenance of artifacts and services used to enable the interchange of information. Key artifacts include data formats and models, mediation components, interoperability services, and interface specifications.

A53351 Define Interoperability Specifications: This activity includes tasks to define constructs requirements for ensuring consistent and standardized data interchange, both within communities and between organizations and mission areas. Specifications for successful interoperability will include knowledge of Key Interface Profiles for interchange functions, definitions for data sharing services and access layers, formats and canonical representations for shared data, and mediation components for transformation and translation scenarios.

A533511 Identify Key Interface Profiles: This activity identifies all boundaries between organizations, technology, networks, and architectural layers over which data interchange must occur. The identification of applicable Key Interface Profiles (KIPs) for interoperability provides organizations and communities a definitive indication of well-defined interfaces to consider, and ensures higher levels of order, visibility, and stability for data interchange scenarios.

A533512 Define Service and Interface Specifications: This activity defines metadata-based contracts and syntactic/semantic interface constructs to control the discovery and consumption of service-based data assets within the operating environment. These interfaces form the basis for functional interoperability between services that produce data and the capabilities that will consume them.

A533513 Define Models/Schemas: This activity defines common information models and shared formats that provide a canonical data representation between multiple data sources or systems.   Models and metadata schemas enable information integration scenarios for communities and reduce the incidence of tightly-coupled point-to-point interfaces between applications and disparate data repositories.

A533514 Define Translations/Transformations: This activity develops the means to change information content, format, and representation of data to support interoperability among for known and unanticipated consumers. This includes mediation components that provide a master transformation guideline or schema to support unanticipated use as well as explicit translation specifications for known, required data interchange scenarios.

A53352 Maintain Interoperability Components: This activity includes tasks for managing the deployment, operation, and modification of published service interfaces or interoperability metadata. This ensures that anticipated levels of quality, compatibility, and version management are observed, and that ongoing extensions of or modifications to defined interoperability elements and models will not introduce breaking changes to current or ongoing consumers.

A5336 Manage Data Access Mechanisms: This activity involves determining the appropriate method for providing access to data assets in "shared space" (e.g. web service, information sharing application, web page/portal, etc.) and developing the appropriate mechanism. Once developed, these mechanisms will need to be monitored and maintained to ensure accessibility of data assets.

A53361 Define Data Access Mechanisms: This activity translates a well-defined need for data access into the appropriate data access mechanism design specifications. This design should account for both the need for "human" users and the need for "computer" users to access data.

A53362 Maintain Data Access Mechanisms: This activity supports the ongoing configuration management and maintenance of developed data access mechanisms. This includes the monitoring of data access mechanisms to facilitate compliance to required service levels.

A534 Manage Cryptographic Services Infrastructure: This activity consists of planning, organizing, coordinating, and controlling the infrastructure and policy of cryptographic materials and devices. It focuses on the provisioning, storage, invocation, employment, and disposition of cryptographic material and devices. It also provides key recovery capabilities. It takes relevant notifications, policy, and recovery requirements as inputs. This activity produces cryptographic services, policies, and recovered data keys as output. Its controls encompass cryptographic current policy, requests for services, materials, and products. It is enabled by the cryptographic support infrastructure (CSI) and key escrow services.

A5341 Manage Cryptographic Support Infrastructure: This activity focuses on managing the infrastructure supporting lifecycle provisioning, storage, activation, use, and disposition of cryptographic material (hardware and software to include devices, private and public keys, cryptographic algorithms, and key recovery capabilities).   It addresses management and control of cryptographic materials and devices for the information environment. It addresses management of the tracking and inventory control of cryptographic materials issued for use in individual devices for authenticating individual users. It includes management oversight of the operation of trust hierarchies to support net-centric operations.

A53411 Manage Key Ordering Services: This activity manages the resources that are employed within the information environment to order cryptographic key both for initial capability and for re-key.

A53412 Manage Key Generation Services: This activity manages the resources which perform two principal functions: the generation of the key values; and the process known as "Key Production" whereby the key values produced are transformed into the formats needed for distribution to the consumer.

A53413 Manage Key Distribution Services: This activity manages the secure delivery of keys to consumers and any activation processes necessary to prepare a key for use after delivery.

A53414 **Manage Key Management Support Services**: This activity manages the services that are necessary to maintain cryptographic basis for the security of the information environment and to facilitate its efficient operation. These services include: Key Management Infrastructure (KMI) Policy; trust extension; archiving; tracking, control, and accounting; key and data recovery; compromise management and revocation; directory; audit; and product definition.

A53415 **Manage Cryptographic Account Management Services**: This activity manages the activities by which cryptographic material accounts are established for registered users.

A5342 **Manage Cryptographic Materials and Devices**: This activity directs and controls the lifecycle use of cryptographic material (e.g., keying material, specialized keys, and algorithms) and devices from ordering to destruction. This activity is performed by NetOps personnel specifically qualified for cryptographic material management. It is controlled by cryptographic material management policy, guidance, and procedures. It uses the Cryptographic Material Call-out as its basis for issuing material. It enables cryptographically based protection and assurance capabilities during both the use of the material and during the destruction of relinquished material or equipment after the material or equipment is no longer employed. This activity may require both physical material and system-identified material inventories. These inventories must be audited as specified by cryptographic material management policy.

A53421 **Register Identity**: This activity manages the submission of user identity information for use in Public Key Infrastructure (PKI) certificates. User registration is necessary prior to the ordering of cryptographic material or devices. This activity also manages the registration of end-unit devices that will receive over-the-air key material.

A53422 **Order Cryptographic Material or Devices**: This activity defines and documents the unit-level requirements for cryptographic materials and services. The needs of individual units are independently forwarded to Client Nodes for consolidation and forwarding to the PRSN, which coordinates with PSN to satisfy the unit requests. This is an auditable activity.

A53423 **Distribute Cryptographic Material or Devices**: This activity directs and controls the transfer of cryptographic material or devices from staging to the employing units and emplacement of the materials or devices for operational use upon activation. This activity also provides for the return of relinquished cryptographic material or devices to staging locations. The distribution of cryptographic material is carefully audited and reported to the PRSNs.

A53424 **Load and Activate Cryptographic Material or Devices**: This activity manages the process of inserting cryptographic material into operational devices for use and the subsequent invocation of that cryptographic material for operational use. This is an auditable activity.

A53425 **Surrender Cryptographic Material or Devices**: This activity manages the termination of use of cryptographic material by a using unit and either the transfer of the cryptographic material out of user control (via Distribute) or its elimination (via Destroy). This is an auditable activity.

A53426 **Destroy Cryptographic Material or Devices**: This activity manages the rendering of cryptographic material or devices into an unusable and unrecoverable state. It ensures no sensitive data is left unencrypted or intact. The destruction of cryptographic material is carefully audited and reported to the PRSNs.

A5343 **Manage Cryptographic Policy**: This activity ensures the continuous availability of current direction and guidance on the use of cryptographic materials and devices. This includes development and dissemination of guidance and direction, assessment of threats to cryptographic capabilities, and evaluation of cryptographic posture vulnerability.

A53431 **Maintain Cryptographic Policy**: This activity provides direction and guidance on use of cryptographic capabilities within the information environment. It includes the development, maintenance, and dissemination of guidance and direction for the handling and use of cryptographic materials and equipment. This guidance and direction is based on the relationship between the information protection requirements of the user and the capabilities of the cryptographic materials and devices.

A53432 Analyze Cryptographic Posture Vulnerability: This activity focuses on the assessment of the overall posture of the cryptographic capability to resist attacks against the core encryption/decryption methods employed in cryptographic materials and devices.

A53433 Analyze Intelligence for Cryptographic Threats: This activity focuses the study of intelligence information to determine if an adversary has the physical and/or technical capability to counter the core encryption/decryption methods used within cryptographic materials and devices.

A5344 Provide Data Recovery Key Management: This activity addresses the means to recover encrypted data given lost, damaged, or destroyed keys. Management of data recovery includes the escrowing of recovery keys, the authorization to use escrowed recovery keys, and the successful implementation of data recovery. While this activity is particularly important in public key based cryptography, it applies to all cryptographic keying situations. It may be especially important when cryptographic keying techniques are used for data at rest and for data archiving. Qualified NetOps administrators perform data recovery and the management of data recovery keys. This is an auditable activity.

A535 Manage System and Network Configurations: This activity consists of the planning, organizing, coordinating, and controlling of the arrangement of the elements of protection and monitoring capabilities, system and network controls, and incident recovery actions of the information environment. It is generally performed by NetOps Administrators. It takes configuration orders; status reports; and operational and functional performance requirements as inputs and provides performance capabilities and service and infrastructure controls as outputs. It is controlled by environment standards such as policy and operational guidance. It is enabled by Global Information Grid (GIG) systems and networks; net-centric enterprise services; net-centric Community of Interest (COI) applications and services; GIG NetOps facilities; and GIG NetOps personnel. Technical Security Plans for each individually managed site also shall be managed as part of this activity.

A5351 Configure Protection Capabilities: This activity focuses on establishing, maintaining, and coordinating the software and hardware that protect the information environment's computing and communications resources. It involves setting security parameters of the information environment in accordance with security policy and operational guidance. It includes setting both static and dynamic protection-policy parameters in servers, workstations, and device security management information databases. These parameters ensure protection-policy enforcement for operating systems, database management systems, networks, services, and applications. These protection-policy parameters are applicable to users, system services, and application profiles. The activity also includes configuring crypto devices with keys and algorithms. It takes protection requirements, threat assessments, and vulnerability assessments as inputs and produces protection capabilities to meet general and/or specific threats as output. Specific NetOps Administrators (i.e., Security Administrators) usually perform protection configurations. This activity is controlled by operational and functional performance requirements and configuration orders.

A53511 Implement Protection Policy: This activity implements all mandatory and discretionary protection policies relevant to the Global Information Grid (GIG) enterprise level. It also implements discretionary protection policies within any given administrative domain. Implementation activities include setting parameters in mechanisms used for protection policy enforcement, deployment and configuration of protection devices, and re-configuration activities to meet changes in threat posture, changes in performance capabilities, and/or changes in protection policy (e.g., INFOCON Directives).

A53512 Apply Patches and Upgrades: This activity applies patches that have been provided by commercial vendors and/or internal developers to close identified vulnerabilities or to counter newly identified threats. This activity may be routine or it may be prioritized based on the receipt of an Information Assurance Vulnerability Alert (IAVA) directive. It also applies upgrades to protection mechanisms in the form of configuration data (e.g., new virus signatures, new attack

signatures), in the form of software (new policy enforcement mechanism), or in the form of hardware (new protection device). NetOps administrators perform this activity. Policy, threat posture, identified vulnerabilities, and standard NetOps operating procedures control this activity. Patches and upgrades are inputs to the activity, which produces new protection enforcement capabilities, and IAVA compliance reports.

A53513Maintain Protection Configuration Support Tools: This activity maintains the support tools used for managing protection configurations. These tools may include configuration utilities, configuration audit tools, and configuration analysis tools. These tools must be kept current to meet configuration administration needs.

A53514Maintain Protection Configurations: This activity maintains both static and dynamic protection configurations. It is performed by NetOps administrators and automated capabilities. Individual tasks within this activity may be human-performed, human-directed, human-assisted, and/or automated. A defined protection- configuration plan or directive, and standard NetOps operating procedures control this activity. The output is a new protection configuration state and configuration status reports.

A5352 Configure Monitoring Capabilities: This activity focuses on establishing, maintaining, and coordinating the software and hardware that enable the monitoring of computing and communications operations within the information environment. It includes setting both static and dynamic monitoring-policy parameters in servers, workstations, and device monitoring management information databases and sensors. These parameters pertain to monitoring policy adherence in operating systems, database management systems, networks, services, and applications. It includes establishing anomaly, fault, and intrusion detection capabilities, setting anti-virus signatures, setting performance thresholds, data filters, selective auditing (resource, function, and user), and sensor-analyzer inter-communications parameters; and establishing event fusion-correlation capabilities, alarms/alerts handlers, and situation awareness displays. It also includes dynamic adjustments to the monitoring configurations to meet changes in the operational environment and its emergent threats. NetOps administrators are generally responsible for performing these configurations. This activity produces monitoring capabilities to meet general and/or specific threats. This activity is controlled by operational and functional performance requirements and configuration orders

A53521Configure NetOps Situational Awareness Displays: This activity focuses on configuring workstation displays and large-screen Command, Control, Communications and Computers (C4) Coordination Center displays such that personnel performing individual disciplines within NetOps can both independently and jointly gain rapid situational understanding (Micro and Macro levels) and take unified actions appropriate to the situation. These displays may be static or dynamic. This activity is controlled by individual NetOps performers and by C4 Coordination Center Senior Watch Officers. It takes NetOps situational awareness requirements as an input and outputs NetOps situational awareness capabilities. It is controlled by policy, guidance, and standard operating procedures.

A53522Configure NetOps Management and Reporting Systems: This activity focuses on designing and enabling the information flows to meet the NetOps roles and responsibilities for reporting, monitoring situation status, and responding appropriately to incidents. This includes ensuring that the necessary reporting sources are enabled and that report consolidation occurs to support different levels of NetOps management throughout the information environment. NetOps administrators perform this activity. It is controlled by policy, guidance, and standard operating procedures. It takes NetOps management activity requirements as its input and outputs NetOps management support and reporting capabilities. It is controlled by NetOps policy and guidance, and by standard operating procedures.

A53523Deploy NetOps Monitoring Devices/Mechanisms: This activity places monitoring systems, devices, and/or mechanisms within the Global Information Grid (GIG). Some placements may be dynamic to meet changes in system and network configurations, and changes in threat conditions. Some placements may be static (i.e., permanent positioning). NetOps administrators

perform this task. Monitoring tactics, techniques, and procedures (TTPs); policy; and current threat assessments provide controls for this activity. It takes as input various management-level monitoring requirements and individual system, device, or mechanism monitoring capabilities; and provides from local to enterprise-wide monitoring capabilities.

A53524Maintain Monitoring Configuration Support Tools: This activity maintains the support tools used for managing monitoring configurations. These tools may include configuration utilities, configuration audit tools, and configuration analysis tools. These tools must be kept current to meet configuration administration needs.

A53525Maintain NetOps Monitoring Configurations: This activity maintains both static and dynamic monitoring configurations. It is performed by NetOps administrators, NetOps monitors, and by automated capabilities. Individual tasks within this activity may be human-performed, human-directed, human-assisted, and/or automated. A defined monitoring-configuration plan or directive, and standard NetOps operating procedures control this activity. The output is a new monitoring configuration state and configuration status reports.

A5353 Configure System and Network Controls: This activity focuses on establishing, maintaining, and coordinating the software and hardware operating parameters used by the system and network control mechanisms within the information environment. It involves setting the static and dynamic performance-policy parameters of the information environment in servers, workstations, device performance management information databases, and sensors. These parameters pertain to performance-policy enforcement in operating systems, database management systems, networks, services, and applications. It includes establishing resource service-control parameters, (e.g., service-level agreements, bandwidth allocation, path allocation, channel allocation, memory allocation, processor allocation, storage media allocation, throughput guarantees, service priorities). It takes service control requirements as its input and provides enabled system and network control and operational performance capabilities as its output. It includes administering daily control of the regional electromagnetic spectrum and of the in-theater tactical reach-back capability. Generally, NetOps Administrators perform this activity. This activity is controlled by operational and functional performance requirements and configuration orders.

A53531Configure Networks: This activity focuses on the static and dynamic operating parameters used for Local and Wide Area transmission and switching systems in wired and wireless networks. It performs the configuration of networking components. Configuration management shall adhere to appropriate guidelines for securely installing infrastructure (e.g., Telecommunications Guidelines).

A53532Configure Information Technology Systems and Services: This activity focuses on the static and dynamic operating parameters of computing platforms used for hosting, serving, and/or executing software applications and services. It performs the physical and logical configuration of Information Technology components including hardware, firmware, and software. It performs the physical and logical configuration of data storage media. It performs the physical and logical configuration of enterprise net-centric core services, information content repositories, and Community of Interest (COI)-specific services.

A53533Manage Core Applications: This activity focuses on Joint (Community of Interest [COI]-specific) services and applications that are used globally across the enterprise. These global services and applications are developed and managed centrally, but are provided to widely distributed users throughout the Global Information Grid (GIG). This activity does not develop global services or applications, but rather receives them from a central developer, makes them available to distributed users, and provides the capability to retrieve software updates and patches. This activity takes requirements from the joint-user communities, and deploys common applications and services for joint use within or across COIs.

A53534Perform Day-to-Day Control of Electromagnetic Spectrum in Theater: This activity deals with the electromagnetic spectrum management activities accomplished to support operational activities. Frequency-assignment requests and analyses, de-confliction of spectrum

usage, interference resolution, and operational electromagnetic environmental effects are included. Included are coordination among electromagnetic spectrum users in the area of operation*s,* the Federal Aviation Administration (FAA) or similar host nation activities and electronic warfare activities. Spectrum management activities are often concentrated in Joint Frequency Management Offices (JFMO) in the area of operations, with reporting and consultation with Unified Command, Service, DoD-wide, and host nation spectrum management activities. Units operating equipment employing the electromagnetic spectrum obtain authorization for spectrum use from the JFMO, or Service Spectrum Management Activity.

A5354 Recover From Incident: This activity focuses on re-establishing the software and hardware operating capabilities used within the information environment's computing and communications systems. Recovery focuses on operational restoration using existing system and network resources. This activity includes the human-performed, human-guided, and automatic means for recovering system and network capabilities from the degrading effects of a failure or attack incident. This activity may be performed in concert with other automated response activities while operationally connected or may be performed manually after equipment has been taken off the network. Special care must be taken while recovering to properly preserve evidence where law enforcement investigation may be initiated. The activity of recovery is coordinated with activities responding to the incident to insure minimal interference between recovery and response activities. Recovery activities include restoration of capabilities and, if necessary, reconstitution of the affected portion of the information environment. Recovery has a number of specific options and is dependent upon the overall capabilities for fault tolerance and survivability, and upon the state of effects resulting from a failure or attack incident. However, it basically consists of reconfiguration and/or restart actions specifically tailored to a recovery requirement. It is controlled by response Courses of Action (COAs), expected recovery states, operational and functional performance requirements, and configuration orders, and is performed by NetOps response personnel (i.e., administrators and monitors in response roles). Its input is the state of the information environment's operational capabilities following a failure or attack incident. Its output is the state of the information environment's operational capabilities after recovery actions have been implemented.

A53541 Manage Configuration Activities IAW Selected Response Course of Action: This activity manages the execution processes, priorities, and re-configuration requirements in restoring systems, networks, and NetOps capabilities to a previous operational state or to a state suitable for continued operations. It takes a Course of Action (COA) selected from among alternative COAs that may have been generated in response activities as guidance, and sequences specific configuration activities to be performed. It provides new configuration parameters, where required, to continue to counter the threat(s) that created the failure, incident, or attack effects. Where system and/or network resources have been completely destroyed, this activity manages the execution processes to plan and engineer reconstituted operational capabilities using new resources. This activity provides status reports on the progress of recovery actions and results. NetOps personnel perform this management activity. The activity outputs planning and engineering guidance and directions, configuration guidance and directions, new configuration parameters, and recovery status reports.

A53542 Restore Capabilities: This activity focuses on recovery from failure, damage, or disruption. It manages the Course of Action (COA) for restoration of operational capabilities using existing resources.

A53543 Reconstitute Capabilities: This activity focuses on recovery from destruction. It manages the Course of Action (COA) for reconstitution of operational capabilities using new, or reserve (e.g., Continuity of Operations), resources. If the need is to use new resources, then planning and engineering of operational capabilities must be performed. If the need is to be satisfied through reserve resources, then there may only be the need to bring those resource configurations to a specified operational state (e.g., reload content using backups).

A536   Manage Accounts: This activity consists of (1) managing the identities and attributes; authentication credentials; and authorizations of users; and (2) managing the identities and permitted allocations of resources.   Collectively, these sets of user and resource features comprise an account. Currently, identified types of accounts include user account, role account, Community of Interest (COI) account, collaboration account, resource account, and audit account. Currently, the identified sets of users include user groups, user roles, agents, collectives (e.g., COIs and collaborations), and other principals. It takes requests account information, authentication and authorization data, and system and resource Identifications(IDs) as input and produces accounts, reports, authentications, authorizations and permissions as outputs. This activity is controlled by policies. It is enabled by Global Information Grid (GIG) systems and networks; net-centric enterprise services; net-centric COI applications and services; GIG NetOps facilities; and GIG NetOps personnel.

A5361 Create Accounts: This activity focuses on the establishment of user (principal) accounts and resource accounts. Individual accounts are given unique identifiers to reflect the type of account: user accounts, Community of Interest (COI) accounts, role accounts, collaboration accounts, audit account, and resource accounts. Accounts permit the monitoring and auditing of actions and resource performance within the information environment. Accounts can be composed from other accounts and are monitored (with respect to a specified set of parameters to be observed) over a specified duration of time. Profiles (e.g., user profile, role profile, group profiles) may be linked with or directly incorporated into accounts. Resource accounts are initiated as new resources become available and are activated within the information environment.

A5362 Maintain Accounts: This activity focuses on managing the dynamic nature of accounts, keeping accounts current and operationally relevant in accordance with specified policies and with authorized changes that may be manually or automatically initiated. It administers required changes to accounts such as privileges, identity authentication parameters, resource allocations, and user-profile bindings.

A5363 Close Accounts: This activity terminates accounts to remove users from the information environment. Resource accounts are removed as appropriate to reflect permanent removal of resources from the environment. Upon account termination, the activity may provide audited account data for archival purposes.

A5364 Manage Trust Infrastructure: This activity focuses on managing the policy, infrastructure (nodes, mechanisms, devices, materials, and personnel), and information parameters used for authentication. The trust infrastructure and authentication policy provides the means to verify the authenticity of an identity, . It provides the authentication mechanisms (credential validation/revocation) and the authentication data (e.g., certificates). This activity is performed through the information environment's Trust Establishment Hierarchy. (i.e. Policy Authorities, Root CA, Subordinate CAs). Each CA establishes their own "domain of trust" over a set of resources, people, and information. Relationships among such Trust Domains can be peered and/or hierarchical.

A53641 Manage Principal's Credentials: This activity focuses on actions necessary to create artifacts (credentials) that can be used to authenticate identity rights, and privileges of the bearer of the artifact. This activity includes re-keying the certificate due to end of crypto-period or key compromise.

A53642 Manage Certificate Revocation List (CRL): This activity is focused on ensuring that authentication certificates, once revoked, cannot be used for authentication. Revocation may occur because of lost, stolen, compromised, or damaged certificates. It may also occur as the certificate's end-of-life has been reached. All revocations are posted to a CRL, which is checked during an authentication transaction to validate a given certificate before it is accepted. The Certifying Authority manages this list.

A53643Manage Token and/or Biometric Information: This activity manages token and biometric information in a way that enables the validation of principals' credentials for subsequent authentication purposes. This activity ensures authentication policy is implemented as intended.

A53644Establish Cross-Domain Authentication between Certificate Authorities: This activity establishes trust between certificate authorities. One method of attaining this trust is to use a "bridge certificate" for use between the two authorities. This bridge certificate is used to establish trust between two domains such that a user from one domain can be authenticated and authorized to invoke and execute authorized services in another domain.

A5365 Manage Authorizations: This activity focuses on managing the policy, infrastructure (nodes, mechanisms, devices, materials, and personnel), and information parameters used for authorization. It provides capabilities for enabling/disabling entity permissions, rights, or privileges to perform a service or action directly or on behalf of another entity (e.g., user, proxy, delegated agent). Authorization attributes may be established on either the object to be accessed, on the subject that is accessing the object, or on a combination of both.

A53651Manage System Entry Authorizations: This activity focuses on capabilities for enabling and/or disabling entity permissions, rights, or privileges associated with locally or remotely entering host systems. Permission restrictions may be based on time-of-day, user location, device identity, port identity, etc. Authorization Restriction Parameters may be static or dynamic. NetOps Security Administrators construct this type of authorization based on local and enterprise-wide policy, and deconflict this type of authorization with other types of authorization being employed. This activity is controlled by access and usage policies that respond to evaluated threats.

A53652Manage Authorization Delegation: This activity focuses on managing the means used for one entity to enable/disable permissions for another entity to act on its behalf. Two forms of authorization delegation can be instantiated, full delegation of rights or restricted (or partial) delegation of rights. An example is a proxy, which is another user or user-agent that acts within a restricted set of activities on behalf of the rights-delegating user. Delegating full-rights enables another user or user-agent to perform every action the rights-delegating user can perform. Thus, the management of delegated authorizations must be carefully addressed. This is particularly true if an entity is composed of user rights, agent-delegated rights, role-rights, etc. The goal is to enable information environment use while maintaining least-privilege operations.

A53653Manage Service Access Authorizations: This activity focuses on managing the means used for permitting one entity or its proxy-agent to invoke and execute a specified service capability.

A53654Manage Application Access Authorizations: This activity focuses on managing the means used for permitting one entity or its proxy-agent to invoke and execute a specific application.

A53655Manage Network Access: This activity focuses on managing the means used for permitting one entity or its proxy-agent to access and use a specific network and/or network channel.

A53656Manage Data Access Authorizations: This activity focuses on managing the means used for permitting one entity or its proxy-agent to access and use specific data or sets of data.

A53657Manage Data Import/Export Authorizations: This activity focuses on managing the means used to enable/disable permission for one entity or its proxy-agent to perform information environment data import/export operations.

A53658Manage Data Release Authorizations: This activity focuses on managing the means used to enable/disable permissions that control the release of information. Data release may be controlled on the basis of time, source, provenance, content, maturity, and/or destination.

A5366 Activate Accounts: This activity focuses on selectively activating specific accounts.

A537 Manage Monitoring Activity: This activity focuses on observing and understanding the dynamic performance and operational use of the information environment. Its goal is to create and maintain situational knowledge of the status of the environment's networks and systems to

produce comprehensive situational awareness of the information environment. It conducts assessments of both threats and incidents in order to adjust protection measures within the infrastructure. It also includes providing discrete analysis, assessing potential impact and determining threat mitigation strategies. The activity includes the collection, testing, and analysis of configuration information, and assessment of operational states to detect disruption and degradation that indicate failures or security problems. It tests and analyzes performance and policy enforcement aspects of a given configuration. It audits operational use and detects failures, attack signatures, or anomalous events; and characterizes such events as incidents requiring a response. NetOps Monitors perform this activity. It receives status, performance information, and configuration data of the environment as inputs and produces threat and incident assessments, incident and audit reports, and configuration changes. This activity is controlled by functional and operational performance requirements and configuration test plans. This activity is enabled by NetOps Common Operational Picture (NetCOP).

A5371 Maintain NetOps-Related Threat Assessment: This activity focuses of the fusion, correlation, and analysis of incident information and the current status of the information environment to produce a current threat assessment. It takes as input information from intelligence sources in the form of indications and warnings, and threat assessments. It also receives attack sensing and warning information from intelligence sensors. It produces as output a current threat assessment for the information environment.

A5372 Test Configuration: This activity performs tests according to a test evaluation plan to measure the resulting performance, protection, and monitoring capabilities that ensue from configuration initialization or changes.

A5373 Analyze Configuration: This activity performs the analysis of test results in accordance with a test evaluation plan to assess the measured performance, protection, and monitoring capabilities that ensued from configuration initialization or changes against expected and/or required capability metrics.

A5374 Monitor Operational Use: This activity focuses on maintaining knowledge of the operational status and operational use of system, network, and storage resources within the information environment. This knowledge is acquired by collecting, testing, and analyzing configuration information and by assessing operational use to detect disruption and degradation that indicate failures or security problems. The activity also includes the assessment of threats and the assessment of incidents. In addition to observation, monitoring includes both discrete and continuous analysis, assessing potential impacts, and determining threat mitigation opportunities. It requires the ability to receive user and resource activity status and performance-related information from auditing services and to selectively reduce, digest, fuse, and/or correlate audit data. Such audit-data manipulation operations may require both real-time and off-line capabilities.

A5375 Perform Environment Situation Awareness: This activity focuses on the dynamic capture, fusion, correlation, representation, and display of the information environment's sensor and monitoring data to support awareness of the state of the environment. This activity provides the basis for analysis, cognizance, and decision-making regarding environment operations in support of designated missions. It integrates information from disparate sources, including the user (either obtained by input or automatic sensing) to provide the user with a tailored view, in accordance with the user's profile, of his situation (User may be a producer or consumer, a human or device/system). The activity invokes concurrent core enterprise activities/services, as needed, to satisfy requirements determined from the processing of user request stream. The activity provides feedback status and intermediate/final results to users as appropriate. This activity is controlled by policy and guidance, and is performed by NetOps monitoring and response personnel.

A5376 Perform Help Desk/Customer Support: This activity analyzes environmental situation awareness results and interacts to provide customized help to the user and user agent. The help provided is based upon knowledge of the issue source and associated environment resources.

This activity coordinates with the user agent for personalization of interaction. This activity also provides knowledge and training associated with the information environment, and also supports provision by out-of-band or external communications means.

A538   Manage Response Activity: This activity focuses on the full lifecycle of incident response, from the assessment of an incident to the closure of an incident. Response activities apply triage and response tactics, techniques, and procedures (human-performed, human-directed, or automated) to address failures, outages, attacks, and unauthorized access or misuse of resources. They include immediate and long-term actions initiated to ameliorate or negate the operational consequences of an incident that causes degradation of the information environment's capabilities or performance. These activities determine priorities; identify mitigation opportunities; and correlate, track, and investigate network and systems anomalies. Responses implement defensive and offensive actions to mitigate threats and incidents that affect system and network operations. Responses include hardening the defenses of the systems and/or networks, containment, recovery, restoration, and reconstitution. Those response activities, which yield the restoration of capabilities or performance to pre-event status, are also often referred to as "recovery" continuity of operations (COOP) activities. Response activities also include support of law enforcement/counter-intelligence operations through evidence collection and forensics, diversion and observation of intruders, and trace-back. It also includes the need to coordinate Computer Network Attack operations. It takes incident data and assessments as inputs and results in administrative and prosecutorial actions, and in directed computer network attack actions. This activity is controlled by the operational environment; plans; policies; guidance; laws and regulations; tactics, techniques, and procedures; standards; and funding. It is enabled by Global Information Grid (GIG) systems and networks; net-centric enterprise services; net-centric Community of Interest (COI) applications and services; GIG NetOps facilities; and GIG NetOps personnel.

A5381 Assess Incidents: This activity examines observable or measurable events that occur within the Global Information Grid (GIG) and classifies those events that meet specified thresholds as incidents. Included in this activity is the determination of the system and network effects resulting from an incident and the impacts that such effects have on operational missions.

A5382 Implement Automatic Incident Response: This activity develops courses of action (COA) to respond to failure; anomaly; and attack, misuse, or intrusion incidents. It includes the selection of a specific COA from among the set of alternatives developed, and the execution of that COA. The form of response may be to direct recovery operations, to participate in Law Enforcement/Counter-Intelligence Investigations, or to support Computer Network Attack Operations.

A5383 Participate in Law Enforcement/Counter-Intelligence Investigation: This activity consists of support tasks that enable a Law Enforcement or Counter-Intelligence (CI) Operation to be coordinated and conducted as a response to an incident (e.g., misuse, intrusion, *or* attack) within some portion of the Global Information Grid (GIG). It includes adding additional monitoring instrumentation to the GIG to observe ongoing incidents, the preservation of evidence (both electronically linked and non-linked information), the forensic analysis of that evidence, and the development of a case against the perpetrator(s), who will either be prosecuted or will be subject to command administrative action.

A5384 Support Computer Network Attack Operations: This activity consists of performing support actions as directed by the Computer Network Attack Commander.

A54   Govern Enterprise Information Environment Evolution: This activity aggregates the functions of governing the evolution of the Enterprise Information Environment. This includes activities to govern architecture evolution and data activities.

A541   Govern Net-Centric Architecture Evolution: This activity pertains to the policy, management, and general oversight regarding the development of DoD's Service/Program/ System architectures and implementation plans.

A5411 Control Capability Increment Integration: This activity aggregates the functions of managing all aspects of integrating a new increment of capability within the information environment. Key aspects of control include timing, funding, readiness for implementation, and post-implementation assessments. The input to this activity is the notification for a new capability to be integrated into the information environment and its state of development. Timing of this activity may be made coincident with capability assessments or program milestones. This activity could be as simple as introducing a new application or as complex as introducing a transformational communications capability. GIG governance activities are included as sub-activities within this activity.

A54111 Assess Readiness for Increment Integration: This activity takes a given increment of EIE capability and analyzes and evaluates its inherent performance and assurance prior to integration. It tests all relevant interfaces that enable the integration to ensure they can integrate successfully. The results of this assessment are subsequently used in certifying the fully integrated capability.

A54112 Certify Integrated Capability: This activity uses certification assessment information for a given EIE capability increment and performs additional analyses and assessments to confirm that the integrated capability meets performance and assurance requirements. The output of this activity is used to accredit the integrated result for operations.

A54113 Accredit Integrated Capability for Operation: This activity provides the approval to operate a newly integrated increment of EIE capability. It is performed by a designated accreditation authority and uses increment and increment integration certification information as the basis for approval.

A5412 Govern GIG IT Portfolio Investment: This activity assesses the performance of the current IT portfolio investments against current and future needs and directs changes in funding and/or portfolio contents necessary to ensure the IT portfolio investments are meeting established performance requirements.

A54121 Govern Legacy IT Portfolio Investment: This activity assesses the performance of the legacy components in the current IT portfolio investments (i.e. sustainment and readiness) against current and future needs and directs changes in funding and/or legacy portfolio component contents necessary to ensure the overall IT portfolio investments are meeting established performance requirements.

A54122 Govern Modernization IT Portfolio Investment: This activity assesses the performance of the modernization components in the current IT portfolio investments against current and future needs and directs changes in funding and/or modernization portfolio component contents necessary to ensure the overall IT portfolio investments are meeting established performance requirements.

A542   Institutionalize Net-Centric Data Strategy: The activity supports the institutionalization of the Net-Centric Data Strategy through sustained leadership commitment to developed strategies, policies and plans. Communities should promote and sustain successful data management practices by reviewing and sharing metrics, best practices and incentive structures.

A5421 Govern Data Activities: This activity focuses on the participation in governance activities to support net-centric data asset sharing and enforce data policies within a Community.

A54211 Participate in GIG Governance: This activity includes participation in governance activities that enable net-centric data asset sharing, including: participation in GIG Enterprise Service efforts, Net-Centric architectural compliance and IT Portfolio Management.

A54212 Enforce Net-Centric Data Policies: This activity verifies that the execution of responsibilities and compliance to standards/specifications as specified through policies. Policy compliance may be assessed through formal program reviews, executive/steering level boards or other governing bodies. Additionally, this activity involves the tracking of previously determined metrics and incentives to adjust and redirect strategy/implementation approaches.

A5422 Educate and Promote Net-Centric Data Practices: This activity supports the adoption of Net-Centric data principles by promoting and educating users of their responsibilities and benefits of participation. Best practices show that new operating practices are assimilated more quickly when coupled with promotional and educational activities.   Communities should develop promotional and educational campaigns to facilitate the adoption of Net-Centric Data Strategy goals across the Department of Defense.

A5423 Advocate Data Strategies: This activity involves vetting, publicizing, and institutionalizing the Net-Centric Data Sharing strategies, plans and guidance.

APPENDIX B -- FEA BRM DEFINITIONS FOR DOD EA BRM

FEDERAL LINES OF BUSINESS AND DESCRIPTIONS

This section contains the definitions for all elements represented in the FEA BRM. The definitions are organized in order of the four Business Areas in the BRM: Services for Citizens, Mode of Delivery, Support Delivery of Services, and Management of Government Resources.   The definitions may be used as a reference for the tables in Appendices A-D that map the FEA RM elements to the DoD EA RM elements.

SERVICES FOR CITIZENS

COMMUNITY AND SOCIAL SERVICES- Community and Social Services includes all activities aimed at creating, expanding, or improving community and social development, social relationships, and social services in the United States. This includes all activities aimed at locality-specific or nationwide social development and general social services. This Line of Business includes general community development and social services programs, as well as earned and unearned benefit programs that promote these objectives.

■ Homeownership Promotion- Homeownership promotion includes activities devoted to assisting citizens interested in buying homes and educating the public as to the benefits of homeownership. NOTE: Activities devoted to the provision of housing to low-income members of the public are located in the Housing Assistance Sub-Function.

■ Community and Regional Development - Community and Regional Development involves activities designed to assist communities in preventing and eliminating blight and deterioration, assist economically distressed communities, and encourage and foster economic development through improved public facilities and resources.

■ Social Services- Social Services are designed to provide meaningful opportunities for social and economic growth of the disadvantaged sector of the population in order to develop individuals into productive and self-reliant citizens and promote social equity.   Included in this category are social welfare services extended to children and adults with special needs, such as the orphaned, neglected, abandoned, disabled, etc.   Such services include family life education and counseling, adoption, guardianship, foster family care, rehabilitation services, etc. Note: This Sub-Function does not include services that are primarily for income support (Income Security) or are an integral part of some other Line of Business (e.g., Health, Workforce Management, etc.). For mapping purposes, this category should only include IT systems that support programs mapped to the "Social Services" budget functional classification.

■ Postal Services- Postal Services provide for the timely and consistent exchange and delivery of mail and packages between businesses, organizations, and residents of the United States or between businesses, organizations, and residents of the United States and the rest of the world. It also includes the nation-wide retail infrastructure required to make Postal Services easily accessible to customers. (Note: The commercial function of mail is more closely aligned with the "Business and Industry Development" Sub-Function in the "Economic Development Line of Business." The international commercial function of mail is more closely aligned with the "Global Trade" Sub-Function in the "International Affairs" Line of Business).

DEFENSE AND NATIONAL SECURITY – Protect and advance U.S. national interests and, if deterrence fails, decisively defeat threats to those interests.

■ Strategic National and Theater Defense - Strategic National and Theater Defense involves establishing national and multinational military objectives; sequencing initiatives; defining limits and assess risks for the use of military and other instruments of national power; developing global

plans or theater war plans to achieve these objectives; and providing military forces and other capabilities in accordance with strategic plans.

■ Operational Defense - Operational Defense involves linking tactics and strategy by establishing operational objectives needed to accomplish the strategic objectives, sequencing events to achieve the operational objectives, initiating actions, and applying resources to bring about and sustain these events.

■ Tactical Defense - Tactical Defense involves focusing on the ordered arrangement and maneuver of combat elements in relation to each other and to the enemy to achieve combat objectives.

DISASTER MANAGEMENT- Disaster Management involves the activities required to prepare for, mitigate, respond to, and repair the effects of all disasters whether natural or man-made.

■ Disaster Monitoring and Prediction- Disaster Monitoring and Prediction involves the actions taken to predict when and where a disaster may take place and communicate that information to affected parties. Note: Weather forecasting, while central to Disaster Monitoring and Prediction, is more closely aligned with the "Environmental Monitoring and Forecasting" Sub-Function in the Environmental Management Line of Business.

■ Disaster Preparedness and Planning- Disaster Preparedness and Planning involves the development of response programs to be used in case of a disaster as well as pre-disaster mitigation efforts to minimize the potential for loss of life and property. This involves the development of emergency management programs and activities as well as staffing and equipping regional response centers, and mitigation-focused construction and preparation.

■ Disaster Repair and Restore- Disaster Repair and Restore involves the cleanup and restoration activities that take place after a disaster. This involves the cleanup and rebuilding of homes, buildings, roads, environmental resources, or infrastructure that may be damaged due to a disaster.

■ Emergency Response- Emergency Response involves the immediate actions taken to respond to a disaster. These actions include, but are not limited to, providing mobile telecommunications, operational support, power generation, search and rescue, and medical life saving actions.

ECONOMIC DEVELOPMENT- Economic Development includes the activities required to promote commercial/industrial development and to regulate the American financial industry to protect investors. It also includes the management and control of the domestic economy and the money supply, and the protection of intellectual property and innovation.

■ Business and Industry Development – Business and Industry Development supports activities related to the creation of economic and business opportunities and stimulus, and the promotion of financial and economic stability for corporations and citizens involved in different types of business.

■ Industry Sector Income Stabilization – Industry Sector Income Stabilization involves all programs and activities devoted to assisting adversely impacted industrial sectors (farming, commercial transportation, etc.) to ensure the continued availability of their services for the American public and the long-term economic stability of these sectors.

■ Intellectual Property Protection - Intellectual Property Protection involves all activities to protect and promote the ownership of ideas and control over the tangible or virtual representation of those ideas, including inventions and discoveries; literary and artistic works; and symbols, names, images, and designs used in commerce.

■ Financial Sector Oversight- Financial Sector Oversight involves the regulation of private sector firms and markets (stock exchanges, corporations, etc.) to protect investors from fraud, monopolies, and illegal behavior. This also includes deposit protection.

EDUCATION – Education refers to those activities that impart knowledge or understanding of a particular subject to the public. Education can take place at a formal school, college, university or other training program. This Line of Business includes all government programs that promote the education of the public, including both earned and unearned benefit programs.

■ Elementary, Secondary, and Vocational Education- Elementary, secondary, and vocational education refers to the provision of education in elementary subjects (reading and writing and arithmetic); education provided by a high school or college preparatory school; and vocational and technical education and training.

■ Higher Education- Higher Education refers to education beyond the secondary level; specifically, education provided by a college or university.

■ Cultural and Historic Preservation - Cultural and Historic Preservation involves all activities performed by the Federal Government to collect and preserve information and artifacts important to the culture and history of the United States and its citizenry and the education of U.S. citizens and the world.

■ Cultural and Historic Exhibition - Cultural and Historic Exhibition includes all activities undertaken by the U.S. government to promote education through the exhibition of cultural, historical, and other information, archives, art, etc.

ENERGY - Energy refers to all actions performed by the government to ensure the procurement and management of energy resources, including the production, sale and distribution of energy, as well as the management of spent fuel resources. Energy management includes all types of mass-produced energy (e.g., hydroelectric, nuclear, wind, solar, or fossil fuels).   Also included in this Line of Business is the oversight of private industry.

■ Energy Supply- Energy Supply involves all activities devoted to ensuring the availability of an adequate supply of energy for the United States and its citizens.

■ Energy Conservation and Preparedness- Energy Conservation and Preparedness involves protection of energy resources from over-consumption to ensure the continued availability of fuel resources and to promote environmental protection. This Line of Business also includes measures taken to ensure the provision of energy in the event of an emergency.

■ Energy Resource Management - Energy Resource Management involves the management and oversight of energy producing resources including facilities, dams, land, and offshore resources.

■ Energy Production- Energy Production involves the transformation of raw energy resources into useable, deliverable energy.

ENVIRONMENTAL MANAGEMENT - Environmental Management includes all functions required to monitor the environment and weather, determine proper environmental standards and ensure their compliance, and address environmental hazards and contamination.

■ Environmental Monitoring and Forecasting - Environmental Monitoring and Forecasting involves the observation and prediction of environmental conditions. This includes but is not limited to the monitoring and forecasting of water quality, water levels, ice sheets, air quality, regulated and non-regulated emissions, as well as the observation and prediction of weather patterns and conditions.

■ Environmental Remediation - Environmental Remediation supports the immediate and long-term activities associated with the correcting and offsetting of environmental deficiencies or imbalances, including restoration activities.

■ Pollution Prevention and Control – Pollution Prevention and Control includes activities associated with identifying appropriate pollution standards and controlling levels of harmful substances emitted into the soil, water and atmosphere from man-made sources. Environmental mitigation projects are also included in this business line.

LAW ENFORCEMENT - Law Enforcement involves activities to protect people, places, and things from criminal activity resulting from non-compliance with U.S. laws. This includes patrols, undercover operations, response to emergency calls, as well as arrests, raids, and seizures of property.

■ Criminal Apprehension - Criminal apprehension involves activities associated with the tracking, arrest, detention, and transportation of groups or individuals believed to be responsible for committing Federal crimes.

■ Criminal Investigation and Surveillance - Criminal Investigation and Surveillance includes collecting evidence required to determine responsibility for a crime and monitoring and questioning affected parties.

■ Citizen Protection - Citizen Protection involves all activities performed to protect the general population of the United States from criminal activity.

■ Crime Prevention - Crime Prevention entails all efforts designed to create safer communities through the control and reduction of crime by addressing the causes of crime and reducing opportunities for crimes to occur.

■ Leadership Protection - Leadership Protection involves all activities performed to protect the health and well being of the president, vice-president, their families, foreign leaders and dignitaries, and other high-level government officials.

■ Property Protection - Property Protection entails all activities performed to ensure the security of civilian and government property as well as foreign diplomatic missions.

■ Substance Control - Substance Control supports activities associated with the enforcement of laws regarding legal substances (i.e., alcohol and tobacco) and illegal narcotics including trafficking, possession, sale, distribution, and other related activities.

LITIGATION AND JUDICIAL ACTIVITIES- Litigation and Judicial Activities refers to those activities relating to the administration of justice.

■ Judicial Hearings – Judicial Hearings includes activities associated with proceedings (usually by a court of law) where evidence is taken for the purpose of determining an issue of fact and reaching a decision based on that evidence.

■ Legal Defense- Legal Defense includes those activities associated with the representation of a defendant in a criminal or civil proceeding.

■ Legal Investigation- Legal Investigation includes activities associated with gathering information about a given party (government agency, citizen, corporation) that would be admissible in a court of law in an attempt to determine a legal question or matter.

■ Legal Prosecution and Litigation- Legal Prosecution and Litigation includes all activities involved with presenting a case in a legal proceeding both in a criminal or civil court of law in an attempt to prove guilt/responsibility.

■ Resolution Facilitation – Resolution Facilitation refers to those activities outside a court of law, such as mediation and arbitration, that may be used in an attempt to settle a dispute between two or more parties (government agency, citizen, corporation).

CORRECTIONAL ACTIVITIES- Correctional Activities involves all Federal activities that ensure the effective incarceration and rehabilitation of convicted criminals.

■ Criminal Incarceration - Criminal Incarceration includes activities associated with the housing, custody and general care of criminals serving time in penitentiaries.

■ Criminal Rehabilitation - Criminal Rehabilitation includes all government activities devoted to providing convicted criminals with the educational resources and life skills necessary to rejoin society as responsible and contributing members.

HEALTH - Health involves Federal programs and activities to ensure and provide for the health and well being of the public. This includes the direct provision of health care services and immunizations as well as the monitoring and tracking of public health indicators for the

detection of trends and identification of widespread illnesses/diseases. It also includes both earned and unearned health care benefit programs.

■ Illness Prevention - Illness Prevention supports activities associated with the prevention and mitigation of illness and disease.

■ Immunization Management - Immunization Management includes all activities associated with the preparation, storage, and use of inoculations and vaccinations.

■ Public Health Monitoring - Public Health Monitoring involves activities associated with monitoring the public health and tracking the spread of disease.

■ Health Care Services - Health Care Services involves programs and activities that directly provide health and medical care to the American public, including both earned and unearned health care benefit programs.

■ Consumer Health and Safety- Consumer Health and Safety supports activities associated with the inspection, education, and evaluation of consumer products to assess the potential risks and dangers they may present to the consumer (both humans and animals), (i.e. food, cosmetics, pharmaceuticals, and other consumer products).

HOMELAND SECURITY- Homeland Security involves protecting the nation against terrorist attacks. This includes analyzing threats and intelligence, guarding borders and airports, protecting critical infrastructure, and coordinating the response emergencies. The Homeland Security Line of Business is defined by the President's Strategy on Homeland Security. Note: Some of the Critical Mission Areas from the President's strategy have already been identified in other Lines of Business in the BRM.

■ Border and Transportation Security – Border and Transportation Security includes appropriately facilitating or deterring entry and exit of people, goods, and conveyances at and between U.S. ports of entry, as well as ensuring the security of transportation and infrastructure networks, facilities, vehicles, and personnel within the United States.

■ Key Asset and Critical Infrastructure Protection – Key Asset and Critical Infrastructure Protection involves assessing key asset and critical infrastructure vulnerabilities and taking direct action to mitigate vulnerabilities, enhance security, and ensure continuity and necessary redundancy in government operations and personnel.

■ Catastrophic Defense – Catastrophic Defense involves the development of technological countermeasures (chemical, biological, radiological and nuclear [CBRN]) to terrorist threats, conducting laboratory testing on new and promising devices, and conducting basic and applied science that can lead to the development of countermeasures.

INCOME SECURITY – Income Security includes activities designed to ensure that members of the public are provided with the necessary means – both financial and otherwise – to sustain an adequate level of existence. This includes all benefit programs, both earned and unearned, that promote these goals for members of the public.

■ General Retirement and Disability- General Retirement and Disability involves the development and management of retirement benefits, pensions, and income security for those who are retired or disabled.

■ Unemployment Compensation - Unemployment Compensation provides income security to those who are no longer employed, while they seek new employment.

■ Housing Assistance - Housing Assistance involves the development and management programs that provide housing to those who are unable to provide housing for themselves including the rental of single-family or multifamily properties, and the management and operation of federally supported housing properties.

■ Food and Nutrition Assistance- Food and Nutrition Assistance involves the development and management of programs that provide food and nutrition assistance to those members of the public who are unable to provide for these needs themselves.

■ Survivor Compensation- Survivor Compensation provides compensation to the survivors of individuals currently receiving or eligible to receive benefits from the Federal Government. This includes, but is not limited to, survivors such as spouses or children of veterans or wage earners eligible for social security payments.

PROVIDE INTELLIGENCE- The business of collecting and analyzing information to meet the national security challenges of the US by processing reliable, accurate foreign intelligence and disseminating intelligence products to policymakers, military commands, and other consumers.
■ Intelligence Planning and Direction/Needs: Establishing the intelligence requirements of the policymakers -- the President, the NSC, military commanders, and other officials in major departments and governmental agencies.
■ Intelligence Collection: Gathering of raw data from which finished intelligence is produced.
■ Intelligence Processing and Exploitation: Conversion of large amounts of data to a form suitable for the production of finished intelligence to include translation, decryption, and interpretation of information stored on film and magnetic media through the use of highly-refined photographic an electronic processes.
■ Intelligence Analysis and Production: Integration, evaluation, and analysis of all available data and the preparation of a variety of intelligence products.
■ Dissemination: Delivering the intelligence products to consumers.

INTERNATIONAL AFFAIRS AND COMMERCE- International Affairs and Commerce involves the non-military activities that promote U.S. policies and interests beyond our national borders, including the negotiation of conflict resolution, treaties, and agreements. In addition, this function includes: foreign economic development and social/political development; diplomatic relations with other Nations; humanitarian, technical and other developmental assistance to key Nations; and global trade.
■ Foreign Affairs - Foreign Affairs refers to those activities associated with the implementation of foreign policy and diplomatic relations, including the operation of embassies, consulates, and other posts; ongoing membership in international organizations; the development of cooperative frameworks to improve relations with other Nations; and the development of treaties and agreements.
■ International Development and Humanitarian Aid - International Development and Humanitarian Aid refers to those activities related to the implementation of development and humanitarian assistance programs to developing and transitioning countries throughout the world. Development and aid may include technical assistance (the transfer of knowledge and expertise), and the delivery of equipment, commodities and urgent humanitarian assistance including food aid.
■ Global Trade- Global Trade refers to those activities the Federal Government undertakes to advance worldwide economic prosperity by increasing trade through the opening of overseas markets and freeing the flow of goods, services, and capital.

NATURAL RESOURCES - Natural Resources includes all activities involved in conservation planning, land management, and national park/monument tourism that affect the nation's natural and recreational resources, both private and federal. Note: Energy-related natural resources are covered in the Energy Management line of business.
■ Water Resource Management- Water Resource Management includes all activities that promote the effective use and management of the nation's water resources. Notes: Environmental protection of water resources is included in the Environmental Management Line of Business. Hydroelectric energy production is included in the Energy Production Sub-Function.
■ Conservation, Marine and Land Management- Conservation, Marine and Land Management involves the responsibilities of surveying, maintaining, and operating public lands and monuments, as well as activities devoted to ensuring the preservation of land, water, wildlife,

and natural resources, both domestically and internationally. It also includes the sustainable stewardship of natural resources on federally owned/controlled lands for commercial use (mineral mining, grazing, forestry, fishing, etc.).

■ Recreational Resource Management and Tourism- Recreational Resource Management and Tourism involves the management of national parks, monuments, and tourist attractions as well as visitor centers, campsites, and park service facilities.

■ Agricultural Innovation and Services- Agricultural Innovation and Services involves the creation and dissemination of better methods for farming and the development of better and healthier crops.

TRANSPORTATION - Transportation involves all federally supported activities related to the safe passage, conveyance, or transportation of goods and/or people.

■ Air transportation - Air Transportation involves the activities related to the safe passage of passengers or goods through the air. It also includes command and control activities related to the safe movement of aircraft through all phases of flight for commercial and military operations. Note: The protection of air transportation from deliberate attack is included in the Transportation Security Sub-Function in the Homeland Security Line of Business.

■ Ground Transportation - Ground Transportation involves the activities related to ensuring the availability of transit and the safe passage of passengers and goods over land. Note: The protection of ground transportation from deliberate attack is included in the Transportation Security Sub-Function in the Homeland Security Line of Business.

■ Water Transportation - Water Transportation involves the activities related to ensuring the availability of transit and the safe passage of passengers and goods over sea and water. Note: The protection of maritime transportation from deliberate attack is included in the Transportation Security Sub-Function in the Homeland Security Line of Business.

■ Space Operations - Space Operations involves the activities related to the safe launches/missions of passengers or goods into aerospace and includes commercial, scientific, and military operations.

WORKFORCE MANAGEMENT – Workforce Management includes those activities that promote the welfare of the Nation's workforce by improving their working conditions, advancing opportunities for profitable employment, and strengthening free collective bargaining.

■ Training and Employment - Training and Employment includes programs of job or skill training, employment services and placement, and programs to promote the hiring of marginal, unemployed, or low-income workers.

■ Labor Rights Management - Labor Rights Management refers to those activities undertaken to ensure that employees and employers are aware of and comply with all statutes and regulations concerning labor rights, including those pertaining to wages, benefits, safety and health, whistleblower, and nondiscrimination policies.

■ Worker Safety- Worker Safety refers to those activities undertaken to save lives, prevent injuries, and protect the health of America's workers.

GENERAL SCIENCE AND INNOVATION - General Science and Innovation includes all Federal activities to meet the national need to advance knowledge in this area. This includes general research and technology programs, space exploration activities, and other research and technology programs that have diverse goals and cannot be readily classified into another Line of Business or Sub-function.

■ Scientific and Technological Research and Innovation - Scientific Innovation includes all federal activities whose goal is the creation of new scientific and/or technological knowledge as a goal in itself, without a specific link to the other Lines of Business or Sub-Functions of the BRM. NOTE: Research and development programs that directly support another Service for Citizen should not be included here.

■ Space Exploration and Innovation– Space Exploration and Innovation includes all activities devoted to innovations directed at human and robotic space flight and the development and operation of space launch and transportation systems, and the general research and exploration of outer space.

MODE OF DELIVERY

KNOWLEDGE CREATION AND MANAGEMENT – Knowledge Creation and Management involves the programs and activities in which the Federal Government creates or develops a body or set of knowledge, the manipulation and analysis of which can provide inherent benefits for both the Federal and private sector.

■ Research and Development- Research and Development involves the gathering and analysis of data, dissemination of results, and development of new products, methodologies, and ideas.

■ General Purpose Data and Statistics – General Purpose Data and Statistics includes activities performed in providing empirical, numerical, and related data and information pertaining to the current state of the nation in areas such as the economy, labor, weather, international trade, etc.

■ Advising and Consulting- Advising and Consulting involves the guidance and consultative services provided by the Federal Government to support the implementation of a specific Service for Citizen.

■ Knowledge Dissemination – Knowledge Dissemination addresses those instances where the primary method used in delivering a service is through the publishing or broadcasting of information, such as the Voice of America or web-based museums maintained by the Smithsonian. It is not intended to address circumstances where the publication of information is a by-product of the actual mode of delivery. For example, an agency might perform research (the mode of delivery) addressing a particular service for citizen (for example environmental management) and as a result publish a report on the findings. In this instance, the research would be the mode of delivery and publishing the report would be a Support Delivery of Service.

PUBLIC GOODS CREATION & MANAGEMENT – The construction, manufacturing, administration, and/or management of goods, structures, facilities, common resources, etc. used for the general well being of the American public or society at large.

■ Manufacturing- Manufacturing involves all programs and activities in which the Federal Government produces both marketable and non-marketable goods.

■ Construction- Construction involves all programs and activities in which the Federal Government builds or constructs facilities, roads, dams, etc.

■ Public Resources, Facilities, & Infrastructure Management- Public Resources, Facilities & Infrastructure Management involves the management and maintenance of Government-owned capital goods and resources (natural or otherwise) on behalf of the public, usually with benefits to the community at large as well as to the direct user. Examples of facilities and infrastructure include schools, roads, bridges, dams, harbors, and public buildings. Examples of resources include parks, cultural artifacts and art, endangered species, oil reserves, etc.

■ Information Infrastructure Management- Information Infrastructure Management involves the management and stewardship of a type of information by the Federal Government and/or the creation of physical communication infrastructures on behalf of the public in order to facilitate communication. This includes the management of large amounts of information (e.g., environmental and weather data, criminal records, etc.), the creation of information and data standards relating to a specific type of information (patient records), and the creation and management of physical communication infrastructures (networks) on behalf of the public. Note: Information infrastructures for government use are not included here.

REGULATORY COMPLIANCE AND ENFORCEMENT- Regulatory Compliance and Enforcement involves the direct monitoring and oversight of a specific individual, group, industry, or community participating in a regulated activity via market mechanisms, command and control features, or other means to control or govern conduct or behavior.

◼ Inspections & Auditing – Inspections and Auditing involves the methodical examination and review of regulated activities to ensure compliance with standards for regulated activity.

◼ Standard Setting / Reporting Guideline Development – Standard Setting/Reporting Guideline Development involves the establishment of allowable limits associated with a regulated activity and the development of reporting requirements necessary to monitor and control compliance with allowable limits. This includes the development of requirements for product sampling and testing, emissions monitoring and control, incident reporting, financial filings, etc.

◼ Permits and Licensing – Permits and Licensing involves activities associated with granting, revoking, and the overall management of the documented authority necessary to perform a regulated task or function.

DIRECT SERVICES FOR CITIZENS–The delivery of a good or service to (or on behalf of) the citizenry by the Federal Government with no other intervening persons, conditions, or organizations.

◼ Military Operations- TBD

◼ Civilian Operations- Civilian Operations describes the direct provision of a non-military service for the citizen by government employees.

FINANCIAL VEHICLES

Financial Vehicles involve those monetary exchanges or transactions between Federal Government entities as well as between the Federal Government and non-Federal entities as a means to accomplishing a Federal goal or objective.

FEDERAL FINANCIAL ASSISTANCE- The provision of earned and unearned financial or monetary-like benefits to individuals, groups, or corporations

◼ Federal Grants (Non-State)- Federal Grants involve the disbursement of funds by the Federal Government to a non-Federal entity to help fund projects or activities. This includes the processes associated with grant administration, including the publication of funds availability notices, development of the grant application guidance, determination of grantee eligibility, coordination of the peer review/evaluation process for competitive grants, the transfer of funds, and the monitoring/oversight as appropriate.

◼ Direct Transfers to Individuals- Direct Transfers to Individuals involves the disbursement of funds from the Federal Government directly to beneficiaries (individuals or organizations) who satisfy Federal eligibility requirements with no restrictions imposed on the recipient as to how the money is spent. Direct Transfers include both earned and unearned Federal Entitlement programs such as Medicare, Social Security, unemployment benefits, etc.

◼ Subsidies- Subsidies involve Federal Government financial transfers that reduce costs and/or increase revenues of producers.

◼ Tax Credits -Tax Credits allow a special exclusion, exemption, or deduction from gross income or which provide a special credit, a preferential rate of tax, or a deferral of tax liability designed to encourage certain kinds of activities or to aid taxpayers in special circumstances.

TRANSFERS TO STATES AND LOCAL GOVERNMENTS- Transfers to States and Local Governments involves the transfer of funds or financial assistance from the Federal government to State and Local governments and Indian tribes.

◼ Formula Grants - Formula Grants involves the allocation of money to States or their subdivisions in accordance with distribution formulas prescribed by law or administrative regulation, for activities of a continuing nature.

◼ Project/Competitive Grants - Project/Competitive Grants involves the funding, for fixed or known periods, of projects. Project/Competitive grants can include fellowships, scholarships,

research grants, training grants, traineeships, experimental and demonstration grants, evaluation grants, planning grants, technical assistance grants, survey grants, and construction grants.

■ Earmarked Grants - Earmarked Grants involves the distribution of money to State and Local Governments for a named purpose or service usually specifically noted by Congress in appropriations language, or other program authorizing language.

■ State Loans- State Loans involve all disbursement of funds by the Government to a State or Local Government (or Indian Tribe) entity under a contract that requires the repayment of such funds with or without interest.

CREDIT AND INSURANCE – Credit and Insurance involves the use of government funds to cover the subsidy cost of a direct loan or loan guarantee or to protect/indemnify members of the public from financial losses.

■ General Insurance- General Insurance involves providing protection to individuals or entities against specified risks. The specified protection generally involves risks that private sector entities are unable or unwilling to assume or subsidize and where the provision of insurance is necessary to achieve social objectives.

■ Loan Guarantees- Loan guarantees involve any guarantee, insurance, or other pledge with respect to the payment of all or a part of the principal or interest on any debt obligation of a non-Federal borrower to a non-Federal lender, but does not include the insurance of deposits, shares, or other withdrawable accounts in financial institutions.

■ Direct Loans- Direct loans involve a disbursement of funds by the Government to a non-Federal borrower under a contract that requires the repayment of such funds with or without interest.

SUPPORT DELIVERY OF SERVICES

CONTROLS AND OVERSIGHT - Controls and Oversight ensures that the operations and programs of the Federal Government and its external business partners comply with applicable laws and regulations and prevent waste, fraud, and abuse.

■ Corrective Action - Corrective Action involves the enforcement of activities to remedy internal or external programs that have been found non-compliant with a given law, regulation, or policy.

■ Program Evaluation – Program Evaluation involves the analysis of internal and external program effectiveness and the determination of corrective actions as appropriate.

■ Program Monitoring - Program Monitoring involves the data-gathering activities required to determine the effectiveness of internal and external programs and the extent to which they comply with related laws, regulations, and policies.

INTERNAL RISK MANAGEMENT AND MITIGATION - Internal Risk Management and Mitigation involves all activities relating to the processes of analyzing exposure to risk and determining appropriate counter-measures.

■ Contingency Planning - Contingency Planning involves the actions required to plan for, respond to, and mitigate damaging events.

■ Continuity Of Operations - Continuity of Operations involves the activities associated with the identification of critical systems and processes, and the planning and preparation required to ensure that these systems and processes will be available in the event of a catastrophic event.

■ Service Recovery - Service Recovery involves the internal actions necessary to develop a plan for resuming operations after a catastrophic event occurs.

LEGISLATIVE RELATIONS - Legislative Relations involves activities aimed at the development, tracking, and amendment of public laws through the legislative branch of the Federal Government.

■ Legislation Tracking – Legislation Tracking involves monitoring legislation from introduction to enactment.

■ Legislation Testimony - Legislation Testimony involves activities associated with providing testimony/evidence in support of, or opposition to, legislation.

■ Proposal Development – Proposal Development involves drafting proposed legislation that creates or amends laws subject to Congressional action.

■ Congressional Liaison Operations- Congressional Liaison Operations involves all activities associated with supporting the formal relationship between a Federal Agency and the U.S. Congress.

REGULATORY DEVELOPMENT - Regulatory Development involves activities associated developing regulations, policies, and guidance to implement laws.

■ Policy and Guidance Development - Policy and Guidance Development involves the creation and dissemination of guidelines to assist in the interpretation and implementation of regulations.

■ Public Comment Tracking - Public Comment Tracking involves the activities of soliciting, maintaining, and responding to public comments regarding proposed regulations.

■ Regulatory Creation - Regulatory Creation involves the activities of researching and drafting proposed and final regulations.

■ Rule Publication - Rule Publication includes all activities associated with the publication of a proposed or final rule in the Federal Register and Code of Federal Regulations.

PLANNING AND RESOURCE ALLOCATION - Planning and Resource Allocation involves the activities of determining strategic direction, identifying and establishing programs and processes, and allocating resources (capital and labor) among those programs and processes.

■ Budget Formulation - Budget Formulation involves involves all activities undertaken to determine priorities for future spending and to develop an itemized forecast of future funding and expenditures during a targeted period of time. This includes the collection and use of performance information to assess the effectiveness of programs and develop budget priorities.

■ Capital Planning - Capital Planning involves the processes for ensuring that appropriate investments are selected for capital expenditures.

■ Enterprise Architecture - Enterprise Architecture is an established process for describing the current state and defining the target state and transition strategy for an organization's people, processes, and technology.

■ Strategic Planning - Strategic Planning entails the determination of annual and long-term goals and the identification of the best approach for achieving those goals.

■ Budget Execution – Budget Execution involves day-to-day requisitions and obligations for agency expenditures, invoices, billing dispute resolution, reconciliation, service level agreements, and distributions of shared expenses.

■ Workforce Planning- Workforce Planning involves the processes for identifying the workforce competencies required to meet the agency's strategic goals and for developing the strategies to meet these requirements.

■ Management Improvement - Management Improvement includes all efforts to gauge the ongoing efficiency of business processes and identify opportunities for reengineering or restructuring.

PUBLIC AFFAIRS - Public Affairs involves the exchange of information and communication between the Federal Government, citizens and stakeholders in direct support of citizen services, public policy, and/or national interest.

■ Customer Services - Customer Services supports activities associated with providing an agency's customers with information regarding the agency's service offerings and managing the interactions and relationships with those customers.

■ Official Information Dissemination – Official Information Dissemination includes all efforts to provide official government information to external stakeholders through the use of various types of media, such as video, paper, web, etc.

■ Product Outreach - Product Outreach relates to the marketing of government services products, and programs to the general public in an attempt to promote awareness and increase the number of customers/beneficiaries of those services and programs.

■ Public Relations - Public Relations involves the efforts to promote an organization's image through the effective handling of citizen concerns.

REVENUE COLLECTION - Revenue Collection includes the collection of Government income from all sources. Note: Tax collection is accounted for in Taxation Management Sub-Function in the General Government Line of Business.

■ Debt Collection - Debt Collection supports activities associated with the collection of money owed to the U.S. government from both foreign and domestic sources.

■ User Fee Collection -User fee collection involves the collection of fees assessed on individuals or organizations for the provision of Government services and for the use of Government goods or resources (i.e. National Parks).

■ Federal Asset Sales - Federal Asset Sales encompasses the activities associated with the acquisition, oversight, tracking, and sale of non-internal assets managed by the Federal Government with a commercial value and sold to the private sector.

GENERAL GOVERNMENT - General Government involves the general overhead costs of the Federal Government, including legislative and executive activities; provision of central fiscal, personnel, and property activities; and the provision of services that cannot reasonably be classified in any other Line of Business. As a normal rule, all activities reasonably or closely associated with other Lines of Business or Sub-Functions shall be included in those Lines of Business or Sub-Functions rather than listed as a part of general government. This Line of Business is reserved for central government management operations; agency-specific management activities would not be included here.

■ Central Fiscal Operations - Central Fiscal Operations includes the fiscal operations that the Department of Treasury performs on behalf of the Government. Note: Tax-related functions are included within the Taxation Management Sub-Function.

■ Legislative Functions - Legislative functions include the costs of the Legislative Branch except for the Tax Court, the Library of Congress, and the Government Printing Office revolving fund.

■ Executive Functions - Executive Functions involve the Executive Office of the President.

■ Central Property Management - General Property Management involves most of the operations of the General Services Administration.

■ Central Personnel Management - Central Personnel Management involves most of the operating costs of the Office of Personnel Management and related agencies.

■ Taxation Management – Taxation Management includes activities associated with the implementation of the Internal Revenue Code and the collection of taxes in the United States and abroad.

■ Central Records and Statistics Management - Central Records and Statistics Management involves the operations surrounding the management of official documents, statistics, and records for the entire Federal Government. This Sub-Function is intended to include the management of records and statistics for the Federal government as a whole, such as the records management performed by NARA or the statistics and data collection performed by the Bureau of the Census. Note: Many agencies perform records and statistics management for a particular business function and as such should be mapped to that line of business. The Central Records and Statistics Management is intended for functions performed on behalf of the entire Federal government.

MANAGEMENT OF GOVERNMENT RESOURCES

ADMINISTRATIVE MANAGEMENT – Administrative Management involves the day-to-day management and maintenance of the internal infrastructure.
■ Facilities, Fleet, And Equipment Management – Facilities, Fleet, and Equipment Management involves the maintenance, administration, and operation of office buildings, fleets, machinery, and other capital assets that are possessions of the Federal Government.
■ Help Desk Services - Help Desk Services involves the management of a service center to respond to government and contract employees' technical and administrative questions.
■ Security Management - Security Management involves the physical protection of an organization's personnel, assets, and facilities.
■ Travel - Travel involves the activities associated with planning, preparing, and monitoring of business related travel for an organization's employees.
■ Workplace Policy Development And Management - Workplace Policy Development and Management includes all activities required to develop and disseminate workplace policies such as dress codes, time reporting requirements, telecommuting, etc.

FINANCIAL MANAGEMENT – The use of financial information to measure, operate and predict the effectiveness and efficiency of an entity's activities in relation to its objectives. The ability to obtain and use such information is usually characterized by having in place policies, practices, standards, and a system of controls that reliably capture and report activity in a consistent manner.
■ Accounting- Accounting entails accounting for assets, liabilities, fund balances, revenues and expenses associated with the maintenance of Federal funds and expenditure of Federal appropriations (Salaries and Expenses, Operation and Maintenance, Procurement, Working Capital, Trust Funds, etc.), in accordance with applicable Federal standards (FASAB, Treasury, OMB, GAO, etc.).
■ Budget and Finance - Budget and Finance includes the management of the Federal budget process including the development of plans and programs, budgets, and performance outputs and outcomes as well as financing Federal programs and operations through appropriation and apportionment of direct and reimbursable spending authority, fund transfers, investments and other financing mechanisms.
■ Payments - Payments include disbursements of Federal funds, via a variety of mechanisms, to Federal and private individuals, Federal agencies, state, local and international Governments, and the private sector, to effect payment for goods and services, or distribute entitlements, benefits, grants, subsidies, loans, or claims.
■ Collections and Receivables - Collections and Receivables includes deposits, fund transfers, and receipts for sales or service.
■ Asset and Liability Management - Assets and Liability Management provide accounting support for the management of assets and liabilities of the Federal government.
■ Reporting and Information- Reporting and Information includes providing financial information, reporting and analysis of financial transactions.
HUMAN RESOURCE MANAGEMENT - Human Resource Management involves all activities associated with the recruitment and management of personnel.
■ Benefits Management - Benefits Management involves the administration of entitled benefits for Federal personnel such as retirement, medical, disability, and insurance.
■ Personnel Management –Personnel Management involves the general management of the federal workforce, including but not limited to functions such as personnel action processing, employee tracking, position classification and management, discipline/grievance, advancement and awards, labor relations, etc.

■ Payroll Management and Expense Reimbursement - Payroll Management and Expense Reimbursement involves the administration and determination of Federal employee compensation. Note: See Payments Sub-Function for the actual payment of salary and expenses.

■ Resource Training And Development - Resource Training and Development refers to the active building of competencies in staff members through formal, technical, or other means of education.

■ Security Clearance Management - Security Clearance Management refers to the processes associated with ensuring employees, contractors, and others have been approved to enter Federal buildings, utilize Federal services, and access sensitive information. This includes eligibility determination, badge issuance, clearance tracking, and security verification services.

■ Staff Recruitment And Employment - Staff Recruitment and Employment refers to the active marketing and hiring of personnel to capitalize on opportunities and fill vacancies within an organization as well as the activities focused on retaining staff.

INFORMATION AND TECHNOLOGY MANAGEMENT – Information and Technology Management involves the coordination of information technology resources and systems required to support or provide a citizen service.

■ Lifecycle/Change Management – Lifecycle/Change Management involves the processes that facilitate a smooth evolution, composition, and workforce transition of the design and implementation of changes to agency resources such as assets, methodologies, systems, or procedures.

■ System Development - System Development supports all activities associated with the in-house design and development of software applications.

■ System Maintenance - System Maintenance supports all activities associated with the maintenance of in-house designed software applications.

■ IT Infrastructure Maintenance - IT Infrastructure Maintenance involves the planning, design, and maintenance of an IT Infrastructure to effectively support automated needs (i.e. platforms, networks, servers, printers, etc.).

■ IT Security- IT Security involves all functions pertaining to the securing of Federal data and systems through the creation and definition of security policies, procedures and controls covering such services as identification, authentication, and non-repudiation.

■ Record Retention - Records Retention involves the operations surrounding the management of the official documents and records for an agency.

■ Information Management - Information Management involves the coordination of information collection, storage, and dissemination, and destruction as well as managing the policies, guidelines, and standards regarding information management.

SUPPLY CHAIN MANAGEMENT - Supply Chain Management involves the purchasing, tracking, and overall management of goods and services.

■ Goods Acquisition - Goods Acquisition involves the procurement of physical goods, products, and capital assets to be used by the Federal government.

■ Inventory Control - Inventory Control refers to the tracking of information related to procured assets and resources with regard to quantity, quality, and location.

■ Logistics Management - Logistics Management involves the planning and tracking of personnel and their resources in relation to their availability and location.

■ Services Acquisition - Services Acquisition involves the oversight and/or management of contractors and service providers from the private sector.

MAPPING APPENDICES AND GUIDANCE FOR USAGE IN EXHIBIT 300S

Appendices C, D, E, and F that follow provide guidance on how to use them to prepare an Exhibit 300. The four Appendices are based on the four Operational areas of DoD: Warfighting, Business, Intelligence and the Enterprise Information Environment. The Appendices each have two user sections, External and Internal DoD. The External Section is for a user looking into DoD using the FEA BRM as the point of entry into DoD Operations. The Internal Section is for DoD personnel to use as the crosswalk in describing DoD Operations in terms of the FEA BRM.

When filling out an Exhibit 300, the Internal Section of each Appendix is used. The DoD Program manger identifies what DOD Operational Activities that the Program supports, then inserts into the Exhibit 300 table, the FEA BRM counterpart.

The UJTL Strategic National tasks are not included but are available on the Joint Electronic Library at http://www.dtic.mil/doctrine/jel/cjcsd/cjcsm/m350004c.pdf.

APPENDIX C -- WARFIGHTER OPERATIONS

C-1   Introduction

This appendix contains the standard activities that define warfighter operations within the DoD, and aligns these activities with sub-functions contained in the FEA BRM. The standard activities presented here are derived from operational activities described in detail in the Universal Joint Task List Version (UJTL) 4.2 (CJCSM 3500.04C). The UJTL serves as a common language and common reference system for joint force commanders, combat support agencies, operational planners, combat developers, and trainers to communicate mission requirements. For this version of the BRM, the lower-level Strategic National UJTLs were mapped to the FEA BRM sub-functions. The results of the lower-level mapping were rolled up to the high-level Strategic National UJTLs (SN1-9) for the purpose of display. Future versions of the BRM will map the Strategic Theater, Operational, and Tactical UJTLs to the FEA BRM.

The appendix is divided into two sections. The first section is introduction. The second section is intended be used internal to DoD (e.g., by program managers assigned to Domains, Services, and Agencies) to obtain mappings to the FEA BRM sub-functions for Exhibit 300 purposes. The table in this section is organized by the Strategic National task from the UJTL, and shows the corresponding FEA BRM sub-functions. Note that in some instances the Strategic National UJTLs cross the warfighter, intelligence, business, and Enterprise Information Environment domains.

Definitions for the UJTLs are included in the Appendix A; definitions for the FEA BRM sub-functions are in Appendix B.

C-2   Relationship of DoD EA BRM for Warfighter to FEA BRM

Table C-1 shows the relationship of subfunctions in the FEA BRM to warfighter activities in the DoD EA BRM activities. The table is organized by Strategic National UJTLs so that internal DoD users can find corresponding FEA BRM subfunctions.

Table C-1: Relationship Between
DoD EA BRM for Warfighter and FEA BRM

Services for Citizens

DoD EA BRM	FEA BRM
SN1 Conduct Strategic Deployment and Redeployment	Defense and National Security/ Strategic National and Theater Defense
SN1 Conduct Strategic Deployment and Redeployment	Health/Health Care Services
SN1 Conduct Strategic Deployment and Redeployment	Transportation / Air Transportation
SN1 Conduct Strategic Deployment and Redeployment	Transportation / Ground Transportation
SN1 Conduct Strategic Deployment and Redeployment	Transportation / Water Transportation
SN1 Conduct Strategic Deployment and Redeployment	Transportation / Space Operations
SN1 Conduct Strategic Deployment and Redeployment	International Affairs and Commerce / Foreign Affairs
SN2 Develop National Strategic Intelligence, Surveillance, and Reconnaissance	Defense and National Security/ Strategic National and Theater Defense

DoD EA BRM	FEA BRM
SN3 Employ Forces	Defense and National Security / Strategic National and Theater Defense
SN3 Employ Forces	Environmental Management / Environmental Monitoring and Forecasting
SN3 Employ Forces	Environmental Management / Environmental Remediation
SN3 Employ Forces	Homeland Security / Border and Transportation Security
SN3 Employ Forces	Homeland Security / Key Assets and Critical Infrastructure protection
SN3 Employ Forces	International Affairs and Commerce / Foreign Affairs
SN4 Provide Sustainment	Defense and National Security / Strategic National and Theater Defense
SN4 Provide Sustainment	Community and SOcial Services / Community and Regional Development
SN4 Provide Sustainment	Correctional Activities / Criminal Incarceration
SN4 Provide Sustainment	General Science and Innovation / Scientific and Technological Research and Innovation
SN4 Provide Sustainment	General Science and Innovation / Space Exploration and Innovation
SN4 Provide Sustainment	Health / Illness Prevention
SN4 Provide Sustainment	Health / Immunization Management
SN4 Provide Sustainment	Health / Public Health Monitoring
SN4 Provide Sustainment	Health / Health Care Services
SN4 Provide Sustainment	International Affairs and Commerce / Foreign Affairs
SN4 Provide Sustainment	LITIGATION AND JUDICIAL ACTIVITIES / Legal Investigation
SN4 Provide Sustainment	LITIGATION AND JUDICIAL ACTIVITIES / Resolution Facilitation
SN5 Provide Strategic Direction and Integration	Defense and National Security / Strategic National and Theater Defense
SN5 Provide Strategic Direction and Integration	Disaster Management / Emergency Response
SN5 Provide Strategic Direction and Integration	International Affairs and Commerce / Foreign Affairs
SN6 Conduct Mobilization	Defense and National Security / Strategic National and Theater Defense
SN6 Conduct Mobilization	Community and SOcial Services / Community and Regional Development
SN6 Conduct Mobilization	Community and SOcial Services / Social Services
SN6 Conduct Mobilization	Community and SOcial Services / Postal Services
SN6 Conduct Mobilization	Economic Development / Business and Industry Development
SN6 Conduct Mobilization	Economic Development / Industry Sector Income Stabilization

DoD EA BRM	FEA BRM
SN6 Conduct Mobilization	Economic Development / Intellectual Property Protection
SN6 Conduct Mobilization	Health / Immunization Management
SN6 Conduct Mobilization	Health / Health Care Services
SN6 Conduct Mobilization	Transportation / Air Transportation
SN6 Conduct Mobilization	Transportation / Ground Transportation
SN6 Conduct Mobilization	Transportation / Water Transportation
SN6 Conduct Mobilization	Transportation / Space Operations
SN6 Conduct Mobilization	LITIGATION AND JUDICIAL ACTIVITIES / Resolution Facilitation
SN6 Conduct Mobilization	LITIGATION AND JUDICIAL ACTIVITIES / Judicial Hearings
SN6 Conduct Mobilization	LITIGATION AND JUDICIAL ACTIVITIES / Legal Defense
SN6 Conduct Mobilization	LITIGATION AND JUDICIAL ACTIVITIES / Legal Investigation
SN6 Conduct Mobilization	LITIGATION AND JUDICIAL ACTIVITIES / Legal Prosecution and Litigation
SN6 Conduct Mobilization	Law Enforcement / Criminal Apprehension
SN6 Conduct Mobilization	Law Enforcement / Criminal Investigation and Surveillance
SN6 Conduct Mobilization	Law Enforcement / Citizen Protection
SN6 Conduct Mobilization	Law Enforcement / Crime Prevention
SN6 Conduct Mobilization	Law Enforcement / Property Protection
SN6 Conduct Mobilization	Law Enforcement / Substance Control
SN7 Conduct Force Development	Defense and National Security / Strategic National and Theater Defense
SN8 Foster Multinational and Interagency Relations	Defense and National Security / Strategic National and Theater Defense
SN8 Foster Multinational and Interagency Relations	Community and SOcial Services / Community and Regional Development
SN8 Foster Multinational and Interagency Relations	Community and SOcial Services / Social Services
SN8 Foster Multinational and Interagency Relations	Community and SOcial Services / Postal Services
SN8 Foster Multinational and Interagency Relations	Disaster Management Disaster Monitoring and Prediction
SN8 Foster Multinational and Interagency Relations	Disaster Management / Disaster Preparedness and Planning
SN8 Foster Multinational and Interagency Relations	Disaster Management / Disaster Repair and Restore
SN8 Foster Multinational and Interagency Relations	Disaster Management / Emergency Response
SN8 Foster Multinational and Interagency Relations	Economic Development / Business and Industry Development

DoD EA BRM	FEA BRM
SN8 Foster Multinational and Interagency Relations	Economic Development / Industry Sector Income Stabilization
SN8 Foster Multinational and Interagency Relations	Economic Development / Intellectual Property Protection
SN8 Foster Multinational and Interagency Relations	Economic Development / Financial Sector Oversight
SN8 Foster Multinational and Interagency Relations	Education / Elementary, Secondary, and Vocational Education
SN8 Foster Multinational and Interagency Relations	Education / Higher Education
SN8 Foster Multinational and Interagency Relations	Energy / Energy Supply
SN8 Foster Multinational and Interagency Relations	Energy / Energy Resource Management
SN8 Foster Multinational and Interagency Relations	Energy / Energy Production
SN8 Foster Multinational and Interagency Relations	Environmental Management / Environmental Monitoring and Forecasting
SN8 Foster Multinational and Interagency Relations	Environmental Management / Environmental Remediation
SN8 Foster Multinational and Interagency Relations	Environmental Management / Pollution Prevention and Control
SN8 Foster Multinational and Interagency Relations	General Science and Innovation / Space Exploration and Innovation
SN8 Foster Multinational and Interagency Relations	Health / Illness Prevention
SN8 Foster Multinational and Interagency Relations	Health / Immunization Management
SN8 Foster Multinational and Interagency Relations	Health / Public Health Monitoring
SN8 Foster Multinational and Interagency Relations	Health / Health Care Services
SN8 Foster Multinational and Interagency Relations	Health / Consumer Health and Safety
SN8 Foster Multinational and Interagency Relations	Homeland Security / Border and Transportation Security
SN8 Foster Multinational and Interagency Relations	Homeland Security / Catastrophic Defense
SN8 Foster Multinational and Interagency Relations	Homeland Security / Key Asset and Infrastructure Protection
SN8 Foster Multinational and Interagency Relations	International Affairs and Commerce / Foreign Affairs
SN8 Foster Multinational and Interagency Relations	International Affairs and Commerce / International Development and Humanitarian Aid
SN8 Foster Multinational and Interagency Relations	International Affairs and Commerce / Global Trade
SN8 Foster Multinational and Interagency Relations	Law Enforcement / Criminal Apprehension
SN8 Foster Multinational and Interagency Relations	Law Enforcement / Criminal Investigation and Surveillance
SN8 Foster Multinational and Interagency Relations	Law Enforcement / Citizen Protection
SN8 Foster Multinational and Interagency Relations	Law Enforcement / Crime Prevention
SN8 Foster Multinational and Interagency Relations	Law Enforcement / Leadership Protection

DoD EA BRM	FEA BRM
SN8 Foster Multinational and Interagency Relations	Law Enforcement / Property Protection
SN8 Foster Multinational and Interagency Relations	Law Enforcement / Substance Control
SN8 Foster Multinational and Interagency Relations	Litigation and Judicial Activities/ Legal Investigation
SN8 Foster Multinational and Interagency Relations	Litigation and Judicial Activities / Legal Prosecution and Litigation
SN8 Foster Multinational and Interagency Relations	Natural Resources / Water Resource Management
SN8 Foster Multinational and Interagency Relations	Natural Resources / Recreational Resource Management and Tourism
SN8 Foster Multinational and Interagency Relations	Natural Resources / Agricultural Innovation and Services
SN8 Foster Multinational and Interagency Relations	Transportation / Air Transportation
SN8 Foster Multinational and Interagency Relations	Transportation / Ground Transportation
SN8 Foster Multinational and Interagency Relations	Transportation / Water Transportation
SN8 Foster Multinational and Interagency Relations	Transportation / Space Operations
SN9 Manage Strategic Deterrence of CBRNE Weapons	Defense and National Security / Strategic National and Theater Defense
SN9 Manage Strategic Deterrence of CBRNE Weapons	Disaster Management / Disaster Repair and Restore
SN9 Manage Strategic Deterrence of CBRNE Weapons	Environmental Management / Environmental Remediation
SN9 Manage Strategic Deterrence of CBRNE Weapons	Homeland Security / Key Asset and Critical Infrastructure Protection
SN9 Manage Strategic Deterrence of CBRNE Weapons	International Affairs and Commerce / Foreign Affairs
OP UJTLs	Defense and National Security / Operational Defense
TA UJTLs	Defense and National Security / Tactical Defense

Mode of Delivery

DoD EA BRM	FEA BRM
SN1 Conduct Strategic Deployment and Redeployment	Direct Services for Citizens/Military Operations
SN2 Develop National Strategic Intelligence, Surveillance, and Reconnaissance	Direct Services for Citizens/Military Operations
SN3 Employ Forces	Direct Services for Citizens/Military Operations
SN4 Provide Sustainment	Direct Services for Citizens/Military Operations
SN5 Provide Strategic Direction and Integration	Direct Services for Citizens/Military Operations
SN6 Conduct Mobilization	Direct Services for Citizens/Military Operations
SN7 Conduct Force Development	Knowledge Creation and Management/Research and Development
SN7 Conduct Force Development	Direct Services for Citizens/Military Operations
SN8 Foster Multinational and Interagency Relations	Direct Services for Citizens/Military Operations
SN9 Manage Strategic Deterrence of CBRNE Weapons	Direct Services for Citizens/Military Operations

Support Delivery of Services

DoD EA BRM	FEA BRM
SN1 Conduct Strategic Deployment and Redeployment	N/A
SN2 Develop National Strategic Intelligence, Surveillance, and Reconnaissance	N/A
SN3 Employ Forces	Planning and Resource Allocation/Strategic Planning
SN3 Employ Forces	Planning and Resource Allocation/Workforce Planning
SN4 Provide Sustainment	Planning and Resource Allocation/Capital Planning
SN4 Provide Sustainment	Planning and Resource Allocation/Strategic Planning
SN4 Provide Sustainment	Planning and Resource Allocation/Workforce Planning
SN4 Provide Sustainment	Planning and Resource Allocation/Management Improvement
SN4 Provide Sustainment	Planning and Resource Allocation/Budget Execution
SN4 Provide Sustainment	Planning and Resource Allocation/Budget Formulation
SN5 Provide Strategic Direction and Integration	Planning and Resource Allocation/Budget Formulation
SN5 Provide Strategic Direction and Integration	Planning and Resource Allocation/Capital Planning
SN5 Provide Strategic Direction and Integration	Planning and Resource Allocation/Enterprise Architecture
SN5 Provide Strategic Direction and Integration	Planning and Resource Allocation/Management Improvement
SN5 Provide Strategic Direction and Integration	Planning and Resource Allocation/Strategic Planning
SN5 Provide Strategic Direction and Integration	Planning and Resource Allocation/Workforce Planning
SN5 Provide Strategic Direction and Integration	Public Affairs/Customer Service
SN5 Provide Strategic Direction and Integration	Public Affairs/Official Information Dissemination
SN5 Provide Strategic Direction and Integration	Public Affairs/Product Outreach
SN5 Provide Strategic Direction and Integration	Public Affairs/Public Relations
SN6 Conduct Mobilization	Planning and Resource Allocation/Strategic Planning
SN6 Conduct Mobilization	Planning and Resource Allocation/Workforce Planning
SN6 Conduct Mobilization	Controls and Oversight/ Program Evaluation
SN6 Conduct Mobilization	Planning and Resource Allocation/Capital Planning
SN6 Conduct Mobilization	Public Affairs/Customer Service
SN7 Conduct Force Development	Planning and Resource Allocation/Strategic Planning
SN7 Conduct Force Development	Planning and Resource Allocation/ Enterprise Architecture
SN7 Conduct Force Development	Planning and Resource Allocation/ Management Improvement
SN7 Conduct Force Development	Planning and Resource Allocation /Budget Formulation
SN7 Conduct Force Development	Planning and Resource Allocation/Capital Planning
SN7 Conduct Force Development	Planning and Resource Allocation/Workforce Planning
SN8 Foster Multinational and Interagency Relations	Internal Risk Management and Mitigation/Service Recovery
SN9 Manage Strategic Deterrence of CBRNE Weapons	N/A

Management of Government Resources

DoD EA BRM	FEA BRM
SN1 Conduct Strategic Deployment and Redeployment	Administrative Management/ Facilities, Fleet, and Equipment Management
SN1 Conduct Strategic Deployment and Redeployment	Administrative Management/ Travel
SN1 Conduct Strategic Deployment and Redeployment	Information and Technology Management /Information Management
SN1 Conduct Strategic Deployment and Redeployment	Supply Chain Management/ Logistics Management
SN2 Develop National Strategic Intelligence, Surveillance, and Reconnaissance	N/A
SN3 Employ Forces	Administrative Management/ Travel
SN3 Employ Forces	Human Resource Management/ Personnel Management
SN3 Employ Forces	Information and Technology Management/ IT Security
SN4 Provide Sustainment	Administrative Management/Facilities, Fleet, and Equipment Management
SN4 Provide Sustainment	Administrative Management/ Travel
SN4 Provide Sustainment	Financial Management/Asset and Liability Management
SN4 Provide Sustainment	Financial Management/ Budget and Finance
SN4 Provide Sustainment	Financial Management/ Collections and Receivables
SN4 Provide Sustainment	Financial Management/ Payments
SN4 Provide Sustainment	Financial Management/ Reporting and Information
SN4 Provide Sustainment	Human Resource Management/ Benefits Management
SN4 Provide Sustainment	Human Resource Management/ Payroll Management and Expense Reimbursement
SN4 Provide Sustainment	Human Resource Management /Personnel Management
SN4 Provide Sustainment	Human Resource Management /Resource Training and Development
SN4 Provide Sustainment	Human Resource Management /Security Clearance Management
SN4 Provide Sustainment	Human Resource Management /Staff Recruitment and Employment
SN4 Provide Sustainment	Supply Chain Management/Goods Acquisition
SN4 Provide Sustainment	Supply Chain Management/ Inventory Control
SN4 Provide Sustainment	Supply Chain Management/ Logistics Management
SN4 Provide Sustainment	Supply Chain Management/ Services Acquisition
SN5 Provide Strategic Direction and Integration	Financial Management/ Budget and Finance
	Information and Technology Management/Information Management
SN5 Provide Strategic Direction and Integration	Information and Technology Management/IT Infrastructure Maintenance
SN5 Provide Strategic Direction and Integration	Information and Technology Management/IT Security
SN5 Provide Strategic Direction and Integration	Information and Technology Management/Record Retention
SN5 Provide Strategic Direction and Integration	Supply Chain Management/ Logistics Management
SN6 Conduct Mobilization	Administrative Management/ Facilities, Fleet, and Equipment Management
SN6 Conduct Mobilization	Administrative Management/ Travel
SN6 Conduct Mobilization	Human Resource Management/Benefits Management

DoD EA BRM	FEA BRM
SN6 Conduct Mobilization	Human Resource Management/Payroll Management and Expense Reimbursement
SN6 Conduct Mobilization	Human Resource Management/Personnel Management
SN6 Conduct Mobilization	Human Resource Management/Resource Training and Development
SN6 Conduct Mobilization	Human Resource Management/Security Clearance Management
SN6 Conduct Mobilization	Information and Technology Management/Information Management
SN6 Conduct Mobilization	Supply Chain Management/ Goods Acquisition
SN6 Conduct Mobilization	Supply Chain Management/ Inventory Control
SN6 Conduct Mobilization	Supply Chain Management/ Logistics Management
SN6 Conduct Mobilization	Supply Chain Management/ Services Acquisition
SN7 Conduct Force Development	Human Resource Management/ Resource Training and Development
SN7 Conduct Force Development	Information and Technology Management/IT Infrastructure Maintenance
SN7 Conduct Force Development	Information and Technology Management/ Lifecycle/Change Management
SN7 Conduct Force Development	Information and Technology Management/System Development
SN7 Conduct Force Development	Supply Chain Management/Goods Acquisition
SN8 Foster Multinational and Interagency Relations	Human Resources Management/Resource Training and Development
SN8 Foster Multinational and Interagency Relations	Information and Technology Management/Information Management
SN8 Foster Multinational and Interagency Relations	Information and Technology Management/IT Security
SN8 Foster Multinational and Interagency Relations	Supply Chain Management/ Goods Acquisition
SN8 Foster Multinational and Interagency Relations	Supply Chain Management/ Inventory Control
SN8 Foster Multinational and Interagency Relations	Supply Chain Management/ Logistics Management
SN8 Foster Multinational and Interagency Relations	Supply Chain Management/ Services Acquisition
SN9 Manage Strategic Deterrence of CBRNE Weapons	N/A

APPENDIX D -- BUSINESS OPERATIONS

D-1   Introduction

This appendix contains the standard activities that define business operations within the DoD, and aligns these activities with sub-functions contained in the FEA BRM. The standard activities presented here are derived from operational activities modeled and described in detail in the Business Enterprise Architecture (BEA). The BEA is being developed and maintained under the direction of the DoD Business Management Modernization Program (BMMP) as a blueprint to guide and constrain investments in DoD organization, operations, and systems as they relate to or impact business operations. The BEA provides the basis for the planning, development, and implementation of business management systems that comply with Federal mandates and requirements and produce accurate, reliable, timely, and compliant information for DoD decision-makers.

The appendix is divided into two sections. The first section is the introduction. The second section is intended be used internal to DoD (e.g., by program managers assigned to Domains, Services, and Agencies) to obtain mappings to the FEA BRM sub-functions for Exhibit 300 purposes. The table in this section is organized by standard business activity and for each such activity shows the corresponding FEA BRM sub-function.

Definitions for the BEA activities are included in Appendix A; FEA BRM sub-functions are in Appendix B.

D-2   Relationship of DoD EA BRM for Business to FEA BRM

Table D-1 shows the relationship of Sub Functions in the FEA BRM to business activities in the DoD EA BRM. The table is organized by DoD business activities so that internal DoD users can find corresponding FEA BRM Sub Functions. Please refer to the FY06 A-11 FEA Additional Instructions and Guidance document for the descriptions of the Business Areas, Lines of Business and Sub Function denoted by the numbers in the following table. The concatenation of these three numbers into a six (6) digit field is used to populate the last six digits of the unique project identifier in budget submissions with the format "999-999".

Table D-1: Relationship Between
DoD EA BRM for Business and FEA BRM

BEA OV-05 Number	BEA OV-05 Name	Business Area Number	Line of Business Number	Sub Function Number	FEA BRM Sub Function Name
0.0	Manage the Department of Defense Business Mission	4	00	000	Management of Government Resources
1.0	Perform Planning	3	04	000	Planning and Resource Allocation
1.1	Conduct Strategic Planning	3	04	104	Strategic Planning
1.2	Develop Planning and Resource Guidance	3	04	104	Strategic Planning
1.2	Develop Planning and Resource Guidance	3	06	112	Policy and Guidance Development

BEA OV-05 Number	BEA OV-05 Name	Business Area Number	Line of Business Number	Sub Function Number	FEA BRM Sub Function Name
1.3	Formulate Program and Budget	3	04	101	Budget Formulation
1.3	Formulate Program and Budget	4	02	125	Budget and Finance
1.4	Develop Resource and Performance Plan	3	04	106	Workforce Planning
1.4	Develop Resource and Performance Plan	3	04	107	Management Improvement
1.5	Develop Requirements Strategy	3	02	094	Contingency Planning
1.5	Develop Requirements Strategy	3	02	095	Continuity of Operations
1.5	Develop Requirements Strategy	3	02	096	Service Recovery
1.5	Develop Requirements Strategy	3	04	101	Budget Formulation
1.5	Develop Requirements Strategy	3	04	102	Capital Planning
1.5	Develop Requirements Strategy	3	04	106	Workforce Planning
1.6	Allocate Resources	3	01	003	Program Monitoring
1.6	Allocate Resources	3	04	102	Capital Planning
1.6	Allocate Resources	3	04	105	Budget Execution
2.0	Monitor Performance of the Department of Defense Business Mission	4	00	000	Management of Government Resources
3.0	Conduct Sourcing	4	05	000	Supply Chain Management
3.1	Execute Acquisition Strategy	4	05	142	Goods Acquisition
3.1	Execute Acquisition Strategy	4	05	146	Services Acquisition
3.2	Execute Sales and Procurement	3	07	118	Federal Asset Sales
3.2	Execute Sales and Procurement	4	05	142	Goods Acquisition
3.2	Execute Sales and Procurement	4	05	146	Services Acquisition
3.3	Monitor Sales and Procurement	4	02	126	Payments
3.3	Monitor Sales and Procurement	4	02	129	Reporting and Information
3.4	Execute Program Management	3	01	003	Program Monitoring
3.4	Execute Program Management	3	01	091	Corrective Action
3.4	Execute Program Management	3	01	092	Program Evaluation
4.0	Manage Property and Materiel	4	00	000	Management of Government Resources
4.1	Perform Service Base Operations Support	4	01	119	Facilities, Fleet and Equipment Management
4.2	Perform Build and Make and Maintenance and Sustainment Operation	4	01	119	Facilities, Fleet and Equipment Management

BEA OV-05 Number	BEA OV-05 Name	Business Area Number	Line of Business Number	Sub Function Number	FEA BRM Sub Function Name
4.2	Perform Build and Make and Maintenance and Sustainment Operation	4	02	128	Asset and Liability Management
4.3	Deliver Property and Materiel	4	05	144	Inventory Control
4.3	Deliver Property and Materiel	4	05	145	Logistics Management
4.4	Dispose or Return Property and Materiel	4	05	144	Inventory Control
4.4	Dispose or Return Property and Materiel	4	05	145	Logistics Management
5.0	Perform Environment Safety and Occupational Health Service	1	08	000	Environmental Management
5.0	Perform Environment Safety and Occupational Health Service	4	03	000	Human Resource Management
6.0	Perform Human Resources Management	4	03	000	Human Resource Management
6.1	Perform Organizational Management	3	04	106	Workforce Planning
6.1	Perform Organizational Management	4	01	122	Travel
6.1	Perform Organizational Management	4	05	145	Logistics Management
6.2	Perform Personnel and Pay Management	4	03	132	Payroll Management and Expense Reimbursement
6.2	Perform Personnel and Pay Management	4	03	134	Security Clearance Management
6.2	Perform Personnel and Pay Management	4	03	220	Position Classification and Management
6.2	Perform Personnel and Pay Management	4	03	221	Vacancy Tracking
6.2	Perform Personnel and Pay Management	4	03	222	Applicant Intake and Recruiting
6.2	Perform Personnel and Pay Management	4	03	223	Pre-employment (medical, testing, drug testing, etc.)
6.2	Perform Personnel and Pay Management	4	03	224	Training Management
6.2	Perform Personnel and Pay Management	4	03	226	Discipline and Grievance
6.2	Perform Personnel and Pay Management	4	03	227	Random Drug Testing
6.2	Perform Personnel and Pay Management	4	03	228	Labor Relations
6.2	Perform Personnel and Pay Management	4	03	229	Time and Labor Distribution
6.2	Perform Personnel and Pay Management	4	03	230	Evaluation
6.2	Perform Personnel and Pay Management	4	03	231	Personnel Action Processing
6.2	Perform Personnel and Pay Management	4	03	232	Reporting and Metrics
6.3	Manage Benefits	4	03	225	Benefit Administration

BEA OV-05 Number	BEA OV-05 Name	Business Area Number	Line of Business Number	Sub Function Number	FEA BRM Sub Function Name
7.0	Provide Information Management Services	4	04	000	Information and Technology Management
7.1	Provide Knowledge Management Services	2	02	069	Research and Development
7.1	Provide Knowledge Management Services	2	02	070	General Purpose Data and Statistics
7.1	Provide Knowledge Management Services	2	07	088	Project/Competitive Grants
7.2	Perform Reporting	4	02	129	Reporting and Information
7.3	Manage Public Affairs	3	05	111	Public Relations
7.3	Manage Public Affairs	3	06	113	Public Comment Tracking
7.4	Provide Information Assurance Services	4	01	121	Security Management
7.4	Provide Information Assurance Services	4	03	134	Security Clearance Management
7.4	Provide Information Assurance Services	4	04	140	IT Security
7.4	Provide Information Assurance Services	4	04	142	Information Management
8.0	Perform Financial Management	4	02	000	Financial Management
8.1	Analyze Funds Management	3	04	105	Budget Execution
8.1	Analyze Funds Management	4	02	125	Budget and Finance
8.1	Analyze Funds Management	4	02	129	Reporting and Information
8.2	Administer Entitlements and Sales	3	07	117	User Fee Collection
8.2	Administer Entitlements and Sales	3	07	118	Federal Asset Sales
8.2	Administer Entitlements and Sales	4	02	126	Payments
8.2	Administer Entitlements and Sales	4	02	127	Collections and Receivables
8.3	Manage General Ledger Transactions	4	02	124	Accounting
8.3	Manage General Ledger Transactions	4	02	128	Asset and Liability Management
8.3	Manage General Ledger Transactions	4	02	129	Reporting and Information
8.4	Perform Treasury Operations	3	07	116	Debt Collection
8.4	Perform Treasury Operations	4	02	126	Payments
8.4	Perform Treasury Operations	4	02	127	Collections and Receivables
8.5	Perform Cost Accounting	4	02	124	Accounting
8.6	Perform Financial Management Governance	3	06	112	Policy and Guidance Development
8.6	Perform Financial Management Governance	3	06	114	Regulatory Creation
8.6	Perform Financial Management Governance	4	01	123	Workplace Policy Development And Management

<div style="background-color:red; color:white">

APPENDIX E -- INTELLIGENCE OPERATIONS

</div>

E-1   Introduction

This appendix contains the standard activities that define intelligence operations within the DoD, and aligns these activities with sub-functions contained in the FEA BRM. The standard activities presented here are derived from the IC EA.

The appendix is divided into two sections. The first section is the introduction. The second section is intended be used internal to DoD (e.g., by program managers assigned to Domains, Services, and Agencies) to obtain mappings to the FEA BRM sub-functions for Exhibit 300 purposes.

Definitions for the intelligence-related activities are included in the Appendix A; the FEA BRM sub-functions are in Appendix B.

E-2   Relationship of DoD EA BRM for Intelligence to FEA BRM (Internal)

Table E-1 shows the list of intelligence subfunctions for DoD intelligence organizations, such as DIA, NSA, and Service intelligence, for the FEA BRM and the DoD EA BRM. Since the activities for the FEA BRM were provided by the IC through the IC EA, the activities are the same for both, i.e., there is an exact mapping.

Table E-1: Relationship Between
DoD EA BRM for Intelligence and FEA BRM

Services for Citizens

DoD EA BRM	FEA BRM
Intelligence Operations/Intelligence Planning and Direction and Needs	Intelligence Operations/Intelligence Planning and Direction and Needs
Intelligence Operations/Intelligence Collection	Intelligence Operations/Intelligence Collection
Intelligence Operations/Intelligence Processing and Exploitation	Intelligence Operations/Intelligence Processing and Exploitation
Intelligence Operations/Intelligence Analysis and Production	Intelligence Operations/Intelligence Analysis and Production
Intelligence Operations/Intelligence Dissemination	Intelligence Operations/Intelligence Dissemination

Mode of Delivery

DoD EA BRM	FEA BRM
Intelligence Operations (from Services to Citizens)	Direct Services to Citizens/Military Operations

APPENDIX F – ENTERPRISE INFORMATION ENVIRONMENT

F-1   Introduction

This appendix contains the standard activities that define the Enterprise Information Environment (EIE) within the DoD, and aligns these activities with sub-functions contained in the FEA BRM. The EIE activities presented here are derived from the net-centric activities described in detail in NCOW V1.1. The NCOW activity, A5 *Manage Enterprise Information Environment* depicts the functions of the EIE. This EIE Operations and Management element in the NCOW V1.1 is equivalent to a line of business in the FEA BRM.

Although it is not mapped in this appendix, EIE activities also appear in the Strategic National Universal Joint Task List (UJTL) and map to FEA BRM Mode of Delivery/ Information Infrastructure Management and Management of Government Resources/Information and Technology Management elements.

The appendix is divided into two sections. The first section is the introduction. The second section is intended be used internal to DoD (e.g., by program managers assigned to Domains, Services, and Agencies) to obtain mappings to the FEA BRM sub-functions for Exhibit 300 purposes. The table in this section is organized by the NCOW V1.0 A5 activities, and shows the corresponding FEA BRM sub-function.

Definitions for the NCOW RM V1.1 A5 activities are included in Appendix A; the FEA BRM sub-function definitions are included in Appendix B. Note that all definitions for A5 activities are included in Appendix A but only the activities that actually map to FEA BRM activities are included in the mappings.

F-2   Relationship of DoD EA BRM for EIE to FEA BRM (Internal)

Table F-1 shows the relationship of subfunctions in the FEA BRM to EIE activities in the DoD EA BRM. The table is organized by NCOW RM V1.1 activities so that internal DoD users can find corresponding FEA BRM subfunctions.

Table F-1: Relationship Between the DoD EA BRM for Enterprise Information Environment and the FEA BRM

Services for Citizens

DoD EA BRM	FEA BRM
All NCOW A5 activities conducted at Strategic level	Strategic National and Theater Defense
All NCOW A5 activities conducted at Operational level	Operational Defense
All NCOW A5 activities conducted at Tactical level	Tactical Defense
Develop Information Environment Capabilities A52/Plan and Engineer Information Environment Capability Increments A522	Homeland Security/Key Asset and Critical Infrastructure Protection
Develop Information Environment Capabilities A52/ Plan and Engineer Information Environment Capability Increments A522	Disaster Management/Disaster Preparedness and Planning
Manage System and Network Configurations A535/Configure Protection Capabilities A5351	Homeland Security/Key Asset and Critical Infrastructure Protection
Manage System and Network Configurations A535/ Recover from Incident A5354	Disaster Management/Disaster Repair and Restore

DoD EA BRM	FEA BRM
Manage Core Services A5311/Manage Restoration Services A5315	Disaster Management/Disaster Repair and Restore
Manage Accounts A5362	N/A
Manage Cryptographic Services Infrastructure A534/Provide Data Recovery Key Management A5344	Disaster Management/Disaster Repair and Restore
Manage Monitoring Activity A537/Maintain NetOps-Related Threat Assessment A5371	Disaster Management/Disaster Monitoring and Prediction
Manage Monitoring Activity A537/Monitor Operational Use A5374	Disaster Management/Disaster Monitoring and Prediction
Manage Response Activity A538/Implement Automatic Incident Response A5382	Disaster Management/Emergency Response
Manage Response Activity A538	Disaster Management/Disaster Repair and Restore

Mode of Delivery

DoD EA BRM	FEA BRM
Develop Enterprise Information Environment Capabilities A52/Architect Information Environment Service Capabilities A521	Knowledge Creation and Management/Research and Development
Develop Enterprise Information Environment Capabilities A52/ Architect Information Environment Service Capabilities A521	Regulated Activity Management/Standard Setting and Reporting Guideline Development
Manage System and Network Configurations A535/Configure System and Network Controls A5353	Public Goods Creation and Management/Information Infrastructure Management
Manage Core Services A5311/Manage Storage Services A53116	Knowledge Creation and Management/Knowledge Dissemination
Manage Core Services A5311/Manage Messaging Services A53114	Knowledge Creation and Management/Knowledge Dissemination
Manage Services A531	Public Goods Creation and Management/Information Infrastructure Management
Manage Communities of Interest A532	Public Goods Creation and Management/Information Infrastructure Management
Manage Data Infrastructure A533	Public Goods Creation and Management/Information Infrastructure Management
Manage Cryptographic Services Infrastructure A534	Public Goods Creation and Management/Information Infrastructure Management
Manage System and Network Configurations A535	Public Goods Creation and Management/Information Infrastructure Management
Manage Accounts A536	Public Goods Creation and Management/Information Infrastructure Management
Manage Monitoring Activity A537	Public Goods Creation and Management/Information Infrastructure Management

DoD EA BRM	FEA BRM
Manage Response Activity A538	Public Goods Creation and Management/Information Infrastructure Management
All A5 Activities	Direct Services for Citizens/Military Operations

Support Delivery of Services

DoD EA BRM	FEA BRM
Develop Enterprise Information Environment Capabilities A52/Architect Information Environment Service Capabilities A521	Planning and Resource Allocation/Enterprise Architecture
Manage Cryptographic Services Infrastructure A534/Provide Data Recovery Key Management A5344	Internal Risk Management and Mitigation/Service Recovery
Manage Response Activity A538/Implement Automatic Incident Response A5382	Internal Risk Management and Mitigation/Service Recovery

Management of Government Resources

DoD EA BRM	FEA BRM
Develop Enterprise Information Environment Capabilities A52/Architect Information Environment Service Capabilities A521	Information and Technology Management/Lifestyle/Change Management
Develop Information Environment Capabilities A52/Plan and Engineer Information Environment Capability Increments A522	Information and Technology Management/System Development
Manage System and Network Configurations A535/Implement Protection Policy A53511	Information and Technology Management/IT Security
Manage System and Network Configurations A535/Configure System and Network Controls A5353	Information and Technology Management/IT Infrastructure Maintenance
Manage System and Network Configurations A535/Configure System and Network Controls A5353	Information and Technology Management/System Maintenance
Manage Core Services A5311/Manage Storage Services A53116	Information and Technology Management/Record Retention
Manage Core Services A5311/Manage Storage Services A53116	Information and Technology Management/Information Management
Manage Core Services A5311/Manage Messaging Services A53114	Information and Technology Management/Information Management
Manage Core Services A5311/Manage Restoration Services A5315	Information and Technology Management/IT Security
Manage Core Services A5311/Manage Communities of Interest A5312	Information and Technology Management/Information Management
Manage Accounts A5362/Maintain Trust infrastructure A5364	Information and Technology Management/IT Security
Manage Accounts A562/Manage Authorizations A5365	Information and Technology Management/Information Management
Manage Data Infrastructure A533	Information and Technology Management/Information Management
Manage Cryptographic Services Infrastructure A534 Manage Cryptographic Support Infrastructure A5341	Information and Technology Management/IT Security
Manage Cryptographic Services Infrastructure A534/Manage Cryptographic Materials and Devices A5342	Information and Technology Management/IT Security
Manage Cryptographic Services Infrastructure A534/Manage Cryptographic Policy A5343	Information and Technology Management/IT Security

DoD EA BRM	FEA BRM
Manage Monitoring Activity A537/Maintain NetOps-Related Threat Assessment A5371	Information and Technology Management/IT Security
Manage Monitoring Activity A537/Perform Environment Situation Awareness A5375	Information and Technology Management/Information Management
Manage Monitoring Activity A537/Perform Help Desk and Customer Support A5376	Administrative Management/Help Desk Services
Manage Response Activity A538/Assess Incidents A5381	Information and Technology Management/IT Security
Manage Response Activity A538/Implement Automatic Incident Response A5382	Information and Technology Management/IT Security
Govern Net-Centric Architecture Evolution A541	Information and Technology Management/Lifecycle/Change Management